

# ETSI TS 124 229 V11.28.0 (2019-01)



**Digital cellular telecommunications system (Phase 2+) (GSM);  
Universal Mobile Telecommunications System (UMTS);  
LTE;  
IP multimedia call control protocol based on  
Session Initiation Protocol (SIP)  
and Session Description Protocol (SDP);  
Stage 3  
(3GPP TS 24.229 version 11.28.0 Release 11)**



---

**Reference**RTS/TSGC-0124229vbs0

---

---

**Keywords**GSM,LTE,UMTS

---

**ETSI**

---

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

---

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

---

**Important notice**

---

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommiteeSupportStaff.aspx>

---

**Copyright Notification**

---

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2019.

All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

**3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

**oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners

**GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

---

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

---

# Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under <http://webapp.etsi.org/key/queryform.asp>.

---

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Contents

|  |    |
|--|----|
| Intellectual Property Rights .....   | 2  |
| Foreword.....  | 2  |
| Modal verbs terminology.....   | 2  |
| Foreword.....  | 29 |
| 1 Scope .....  | 30 |
| 2 References .....   | 31 |
| 3 Definitions and abbreviations.....   | 42 |
| 3.1 Definitions .....  | 42 |
| 3.2 Abbreviations .....  | 48 |
| 3A Interoperability with different IP-CAN.....                                   | 50 |
| 4 General .....  | 51 |
| 4.1 Conformance of IM CN subsystem entities to SIP, SDP and other protocols..... | 51 |
| 4.2 URI and address assignments.....   | 54 |
| 4.2A Transport mechanisms.....   | 56 |
| 4.2B Security mechanisms.....  | 56 |
| 4.2B.1 Signalling security .....   | 56 |
| 4.2B.2 Media security .....  | 58 |
| 4.3 Routing principles of IM CN subsystem entities.....                          | 59 |
| 4.4 Trust domain .....   | 59 |
| 4.4.1 General.....   | 59 |
| 4.4.2 P-Asserted-Identity .....  | 59 |
| 4.4.3 P-Access-Network-Info .....  | 59 |
| 4.4.4 History-Info .....   | 60 |
| 4.4.5 P-Asserted-Service.....  | 60 |
| 4.4.6 Resource-Priority .....  | 60 |
| 4.4.7 Reason (in a response) .....   | 60 |
| 4.4.8 P-Profile-Key.....   | 60 |
| 4.4.9 P-Served-User.....   | 60 |
| 4.4.10 P-Private-Network-Indication.....   | 60 |
| 4.4.11 P-Early-Media.....  | 61 |
| 4.4.12 CPC and OLI .....   | 61 |
| 4.4.13 Feature-Caps .....  | 61 |
| 4.5 Charging correlation principles for IM CN subsystems .....                   | 61 |
| 4.5.1 Overview .....   | 61 |
| 4.5.2 IM CN subsystem charging identifier (ICID) .....                           | 61 |
| 4.5.2A Related ICID.....   | 62 |
| 4.5.3 Access network charging information .....                                  | 62 |
| 4.5.3.1 General .....  | 62 |
| 4.5.3.2 Access network charging information.....                                 | 62 |
| 4.5.4 Inter operator identifier (IOI).....                                       | 62 |
| 4.5.4A Transit inter operator identifier (Transit IOI) .....                     | 63 |
| 4.5.5 Charging function addresses .....  | 64 |
| 4.5.6 Void .....   | 65 |
| 4.5.7 Loopback-indication parameter .....  | 65 |
| 4.6 Support of local service numbers .....                                       | 65 |
| 4.7 Emergency service .....  | 65 |
| 4.7.1 Introduction.....  | 65 |
| 4.7.2 Emergency calls generated by a UE .....                                    | 65 |
| 4.7.3 Emergency calls generated by an AS.....                                    | 65 |
| 4.7.4 Emergency calls received from an enterprise network .....                  | 66 |
| 4.7.5 Location in emergency calls .....  | 66 |
| 4.8 Void.....  | 67 |
| 4.9 Overlap signalling .....   | 67 |
| 4.9.1 General.....   | 67 |

|            |  |    |
|------------|--|----|
| 4.9.2      | Overlap signalling methods .....   | 67 |
| 4.9.2.1    | In-dialog method .....   | 67 |
| 4.9.2.1.1  | General .....  | 67 |
| 4.9.2.2    | Multiple-INVITE method .....   | 67 |
| 4.9.2.2.1  | General .....  | 67 |
| 4.9.3      | Routeing impacts .....   | 67 |
| 4.9.3.1    | General .....  | 67 |
| 4.9.3.2    | Deterministic routeing.....  | 67 |
| 4.9.3.3    | Digit collection.....  | 68 |
| 4.10       | Dialog correlation for IM CN subsystems.....   | 68 |
| 4.10.1     | General.....   | 68 |
| 4.10.2     | CONF usage.....  | 68 |
| 4.11       | Priority mechanisms .....  | 68 |
| 4.12       | Overload control.....  | 70 |
| 5          | Application usage of SIP .....   | 70 |
| 5.1        | Procedures at the UE .....   | 70 |
| 5.1.0      | General.....   | 70 |
| 5.1.1      | Registration and authentication.....   | 70 |
| 5.1.1.1    | General .....  | 70 |
| 5.1.1.1A   | Parameters contained in the ISIM .....   | 71 |
| 5.1.1.1B   | Parameters provisioned to a UE without ISIM or USIM .....                                  | 72 |
| 5.1.1.1B.1 | Parameters provisioned in the IMC .....  | 72 |
| 5.1.1.1B.2 | Parameters when UE does not contain ISIM, USIM or IMC .....                                | 72 |
| 5.1.1.2    | Initial registration.....  | 72 |
| 5.1.1.2.1  | General .....  | 72 |
| 5.1.1.2.2  | Initial registration using IMS AKA .....   | 76 |
| 5.1.1.2.3  | Initial registration using SIP digest without TLS .....                                    | 77 |
| 5.1.1.2.4  | Initial registration using SIP digest with TLS .....                                       | 78 |
| 5.1.1.2.5  | Initial registration using NASS-IMS bundled authentication.....                            | 78 |
| 5.1.1.2.6  | Initial registration using GPRS-IMS-Bundled authentication .....                           | 79 |
| 5.1.1.3    | Subscription to the registration-state event package .....                                 | 79 |
| 5.1.1.3A   | Void.....  | 80 |
| 5.1.1.4    | User-initiated reregistration and registration of an additional public user identity ..... | 80 |
| 5.1.1.4.1  | General .....  | 80 |
| 5.1.1.4.2  | IMS AKA as a security mechanism.....   | 83 |
| 5.1.1.4.3  | SIP digest without TLS as a security mechanism.....  | 84 |
| 5.1.1.4.4  | SIP digest with TLS as a security mechanism.....   | 84 |
| 5.1.1.4.5  | NASS-IMS bundled authentication as a security mechanism .....                              | 85 |
| 5.1.1.4.6  | GPRS-IMS-Bundled authentication as a security mechanism.....                               | 85 |
| 5.1.1.5    | Authentication .....   | 86 |
| 5.1.1.5.1  | IMS AKA - general .....  | 86 |
| 5.1.1.5.2  | Void.....  | 87 |
| 5.1.1.5.3  | IMS AKA abnormal cases.....  | 87 |
| 5.1.1.5.4  | SIP digest without TLS – general.....  | 88 |
| 5.1.1.5.5  | SIP digest without TLS – abnormal procedures .....   | 88 |
| 5.1.1.5.6  | SIP digest with TLS – general .....  | 88 |
| 5.1.1.5.7  | SIP digest with TLS – abnormal procedures .....  | 89 |
| 5.1.1.5.8  | NASS-IMS bundled authentication – general .....  | 89 |
| 5.1.1.5.9  | NASS-IMS bundled authentication – abnormal procedures.....                                 | 89 |
| 5.1.1.5.10 | GPRS-IMS-Bundled authentication – general.....   | 89 |
| 5.1.1.5.11 | GPRS-IMS-Bundled authentication – abnormal procedures .....                                | 89 |
| 5.1.1.5.12 | Abnormal procedures for all security mechanisms.....                                       | 89 |
| 5.1.1.5A   | Network-initiated re-authentication .....  | 89 |
| 5.1.1.5B   | Change of IPv6 address due to privacy .....  | 89 |
| 5.1.1.6    | User-initiated deregistration.....   | 90 |
| 5.1.1.6.1  | General .....  | 90 |
| 5.1.1.6.2  | IMS AKA as a security mechanism.....   | 92 |
| 5.1.1.6.3  | SIP digest without TLS as a security mechanism.....  | 93 |
| 5.1.1.6.4  | SIP digest with TLS as a security mechanism.....   | 93 |
| 5.1.1.6.5  | NASS-IMS bundled authentication as a security mechanism .....                              | 94 |
| 5.1.1.6.6  | GPRS-IMS-Bundled authentication as a security mechanism.....                               | 94 |

|            |   |     |
|------------|---|-----|
| 5.1.1.7    | Network-initiated deregistration .....  | 94  |
| 5.1.2      | Subscription and notification .....   | 95  |
| 5.1.2.1    | Notification about multiple registered public user identities.....  | 95  |
| 5.1.2.2    | General SUBSCRIBE requirements.....   | 96  |
| 5.1.2A     | Generic procedures applicable to all methods excluding the REGISTER method.....                                 | 96  |
| 5.1.2A.1   | UE-originating case.....  | 96  |
| 5.1.2A.1.1 | General .....   | 96  |
| 5.1.2A.1.2 | Structure of Request-URI .....  | 100 |
| 5.1.2A.1.3 | UE without dial string processing capabilities .....  | 101 |
| 5.1.2A.1.4 | UE with dial string processing capabilities.....  | 101 |
| 5.1.2A.1.5 | Setting the "phone-context" tel URI parameter .....   | 102 |
| 5.1.2A.1.6 | Abnormal cases .....  | 102 |
| 5.1.2A.2   | UE-terminating case.....  | 103 |
| 5.1.3      | Call initiation - UE-originating case .....   | 105 |
| 5.1.3.1    | Initial INVITE request .....  | 105 |
| 5.1.4      | Call initiation - UE-terminating case .....   | 107 |
| 5.1.4.1    | Initial INVITE request .....  | 107 |
| 5.1.5      | Call release.....   | 108 |
| 5.1.6      | Emergency service.....  | 108 |
| 5.1.6.1    | General.....  | 108 |
| 5.1.6.2    | Initial emergency registration.....   | 109 |
| 5.1.6.2A   | New initial emergency registration .....  | 110 |
| 5.1.6.3    | Initial subscription to the registration-state event package .....  | 110 |
| 5.1.6.4    | User-initiated emergency reregistration .....   | 110 |
| 5.1.6.5    | Authentication.....   | 110 |
| 5.1.6.6    | User-initiated emergency deregistration .....   | 110 |
| 5.1.6.7    | Network-initiated emergency deregistration.....   | 110 |
| 5.1.6.8    | Emergency session setup.....  | 110 |
| 5.1.6.8.1  | General .....   | 110 |
| 5.1.6.8.2  | Emergency session set-up in case of no registration .....   | 111 |
| 5.1.6.8.3  | Emergency session set-up within an emergency registration .....   | 113 |
| 5.1.6.8.4  | Emergency session setup within a non-emergency registration .....   | 114 |
| 5.1.6.9    | Emergency session release.....  | 116 |
| 5.1.6.10   | Successful or provisional response to a request not detected by the UE as relating to an emergency session..... | 116 |
| 5.1.7      | Void .....  | 117 |
| 5.1.8      | Void .....  | 117 |
| 5.2        | Procedures at the P-CSCF .....  | 117 |
| 5.2.1      | General.....  | 117 |
| 5.2.2      | Registration.....   | 120 |
| 5.2.2.1    | General .....   | 120 |
| 5.2.2.2    | IMS AKA as a security mechanism .....   | 124 |
| 5.2.2.3    | SIP digest without TLS as a security mechanism .....  | 128 |
| 5.2.2.4    | SIP digest with TLS as a security mechanism.....  | 129 |
| 5.2.2.5    | NASS-IMS bundled authentication as a security mechanism .....   | 131 |
| 5.2.2.6    | GPRS-IMS-Bundled authentication as a security mechanism .....   | 131 |
| 5.2.2.7    | P-CSCF reconfigured to not accept registrations .....   | 132 |
| 5.2.3      | Subscription to the user's registration-state event package .....   | 132 |
| 5.2.3A     | Void.....   | 133 |
| 5.2.3B     | SUBSCRIBE request .....   | 133 |
| 5.2.4      | Registration of multiple public user identities .....   | 133 |
| 5.2.5      | Deregistration .....  | 134 |
| 5.2.5.1    | User-initiated deregistration.....  | 134 |
| 5.2.5.2    | Network-initiated deregistration .....  | 135 |
| 5.2.6      | General treatment for all dialogs and standalone transactions excluding the REGISTER method.....                | 135 |
| 5.2.6.1    | Introduction.....   | 135 |
| 5.2.6.2    | Determination of UE-originated or UE-terminated case.....   | 135 |
| 5.2.6.3    | Requests initiated by the UE .....  | 136 |
| 5.2.6.3.1  | General for all requests.....   | 136 |
| 5.2.6.3.2  | Void.....   | 137 |
| 5.2.6.3.2A | Abnormal cases .....  | 137 |
| 5.2.6.3.3  | Initial request for a dialog.....   | 137 |

|            |  |     |
|------------|--|-----|
| 5.2.6.3.4  | Responses to an initial request for a dialog .....   | 139 |
| 5.2.6.3.5  | Target refresh request for a dialog .....  | 140 |
| 5.2.6.3.6  | Responses to a target refresh request for a dialog .....   | 141 |
| 5.2.6.3.7  | Request for a standalone transaction .....   | 141 |
| 5.2.6.3.8  | Responses to a request for a standalone transaction .....  | 142 |
| 5.2.6.3.9  | Subsequent request other than a target refresh request .....   | 142 |
| 5.2.6.3.10 | Responses to a subsequent request other than a target refresh request .....  | 143 |
| 5.2.6.3.11 | Request for an unknown method that does not relate to an existing dialog .....   | 143 |
| 5.2.6.3.12 | Responses to a request for an unknown method that does not relate to an existing dialog .....  | 144 |
| 5.2.6.4    | Requests terminated by the UE .....  | 144 |
| 5.2.6.4.1  | Void .....   | 144 |
| 5.2.6.4.2  | General for all responses .....  | 144 |
| 5.2.6.4.3  | Initial request for a dialog .....   | 144 |
| 5.2.6.4.4  | Responses to an initial request for a dialog .....   | 145 |
| 5.2.6.4.5  | Target refresh request for a dialog .....  | 146 |
| 5.2.6.4.6  | Responses to a target refresh request for a dialog .....   | 147 |
| 5.2.6.4.7  | Request for a standalone transaction .....   | 148 |
| 5.2.6.4.8  | Responses to a request for a standalone transaction .....  | 148 |
| 5.2.6.4.9  | Subsequent request other than a target refresh request .....   | 149 |
| 5.2.6.4.10 | Responses to a subsequent request other than a target refresh request .....  | 149 |
| 5.2.6.4.11 | Request for an unknown method that does not relate to an existing dialog .....   | 149 |
| 5.2.6.4.12 | Responses to a request for an unknown method that does not relate to an existing dialog .....  | 149 |
| 5.2.7      | Initial INVITE .....   | 150 |
| 5.2.7.1    | Introduction .....   | 150 |
| 5.2.7.2    | UE-originating case .....  | 150 |
| 5.2.7.3    | UE-terminating case .....  | 151 |
| 5.2.7.4    | Access network charging information .....  | 151 |
| 5.2.8      | Call release .....   | 151 |
| 5.2.8.1    | P-CSCF-initiated call release .....  | 151 |
| 5.2.8.1.1  | Cancellation of a session currently being established .....  | 151 |
| 5.2.8.1.2  | Release of an existing session .....   | 152 |
| 5.2.8.1.3  | Abnormal cases .....   | 154 |
| 5.2.8.1.4  | Release of the existing dialogs due to registration expiration and deletion of the security association, IP association or TLS session ..... | 154 |
| 5.2.8.2    | Call release initiated by any other entity .....   | 154 |
| 5.2.8.3    | Session expiration .....   | 154 |
| 5.2.9      | Subsequent requests .....  | 155 |
| 5.2.9.1    | UE-originating case .....  | 155 |
| 5.2.9.2    | UE-terminating case .....  | 155 |
| 5.2.10     | Emergency service .....  | 155 |
| 5.2.10.1   | General .....  | 155 |
| 5.2.10.2   | General treatment for all dialogs and standalone transactions excluding the REGISTER method – requests from an unregistered user .....       | 156 |
| 5.2.10.2A  | General treatment for all dialogs and standalone transactions excluding the REGISTER method – requests to an unregistered user .....         | 157 |
| 5.2.10.3   | General treatment for all dialogs and standalone transactions excluding the REGISTER method after emergency registration .....               | 157 |
| 5.2.10.4   | General treatment for all dialogs and standalone transactions excluding the REGISTER method - non-emergency registration .....               | 159 |
| 5.2.10.5   | Abnormal and rejection cases .....   | 161 |
| 5.2.11     | Void .....   | 162 |
| 5.3        | Procedures at the I-CSCF .....   | 162 |
| 5.3.1      | Registration procedure .....   | 162 |
| 5.3.1.1    | General .....  | 162 |
| 5.3.1.2    | Normal procedures .....  | 162 |
| 5.3.1.3    | Abnormal cases .....   | 163 |
| 5.3.2      | Initial requests .....   | 164 |
| 5.3.2.1    | Normal procedures .....  | 164 |
| 5.3.2.1A   | Originating procedures for requests containing the "orig" parameter .....  | 167 |
| 5.3.2.2    | Abnormal cases .....   | 169 |
| 5.3.3      | Void .....   | 170 |
| 5.3.3.1    | Void .....   | 170 |

|            |   |     |
|------------|---|-----|
| 5.3.3.2    | Void.....   | 170 |
| 5.3.3.3    | Void.....   | 170 |
| 5.3.4      | Void .....  | 170 |
| 5.4        | Procedures at the S-CSCF .....  | 170 |
| 5.4.0      | General.....  | 170 |
| 5.4.1      | Registration and authentication.....  | 170 |
| 5.4.1.1    | Introduction.....   | 170 |
| 5.4.1.2    | Initial registration and user-initiated reregistration .....  | 172 |
| 5.4.1.2.1  | Unprotected REGISTER .....  | 172 |
| 5.4.1.2.1A | Challenge with IMS AKA as security mechanism .....  | 173 |
| 5.4.1.2.1B | Challenge with SIP digest as security mechanism.....  | 174 |
| 5.4.1.2.1C | Challenge with SIP digest with TLS as security mechanism.....   | 174 |
| 5.4.1.2.1D | Initial registration and user-initiated reregistration for NASS-IMS bundled authentication .....                | 174 |
| 5.4.1.2.1E | Initial registration and user-initiated reregistration for GPRS-IMS-Bundled authentication .....                | 175 |
| 5.4.1.2.2  | Protected REGISTER with IMS AKA as a security mechanism.....  | 177 |
| 5.4.1.2.2A | Protected REGISTER with SIP digest as a security mechanism .....  | 180 |
| 5.4.1.2.2B | Protected REGISTER with SIP digest with TLS as a security mechanism.....  | 183 |
| 5.4.1.2.2C | NASS-IMS bundled authentication as a security mechanism .....   | 183 |
| 5.4.1.2.2D | GPRS-IMS-Bundled authentication as a security mechanism.....  | 183 |
| 5.4.1.2.2E | Protected REGISTER – Authentication already performed .....   | 183 |
| 5.4.1.2.2F | Successful registration.....  | 185 |
| 5.4.1.2.3  | Abnormal cases - general .....  | 187 |
| 5.4.1.2.3A | Abnormal cases – IMS AKA as security mechanism.....   | 188 |
| 5.4.1.2.3B | Abnormal cases – SIP digest as security mechanism .....   | 188 |
| 5.4.1.2.3C | Abnormal cases – SIP digest with TLS as security mechanism .....  | 189 |
| 5.4.1.2.3D | Abnormal cases – NASS-IMS bundled authentication as security mechanism.....                                     | 189 |
| 5.4.1.2.3E | Abnormal cases – GPRS-IMS-Bundled authentication as security mechanism.....                                     | 189 |
| 5.4.1.3    | Authentication and reauthentication.....  | 189 |
| 5.4.1.4    | User-initiated deregistration.....  | 189 |
| 5.4.1.4.1  | Normal cases .....  | 189 |
| 5.4.1.4.2  | Abnormal cases - IMS AKA as security mechanism.....   | 191 |
| 5.4.1.4.4  | Abnormal cases – SIP digest with TLS as security mechanism .....  | 191 |
| 5.4.1.4.5  | Abnormal cases – NASS-IMS bundled authentication as security mechanism.....                                     | 191 |
| 5.4.1.4.6  | Abnormal cases – GPRS-IMS-Bundled authentication as security mechanism.....                                     | 191 |
| 5.4.1.5    | Network-initiated deregistration .....  | 191 |
| 5.4.1.6    | Network-initiated reauthentication.....   | 193 |
| 5.4.1.7    | Notification of Application Servers about registration status .....   | 194 |
| 5.4.1.7A   | Including contents in the body of the third-party REGISTER request.....   | 195 |
| 5.4.1.8    | Service profile updates.....  | 196 |
| 5.4.2      | Subscription and notification .....   | 196 |
| 5.4.2.1    | Subscriptions to S-CSCF events .....  | 196 |
| 5.4.2.1.1  | Subscription to the event providing registration state.....   | 196 |
| 5.4.2.1.2  | Notification about registration state.....  | 198 |
| 5.4.2.1.3  | Void.....   | 202 |
| 5.4.2.1.4  | Void.....   | 202 |
| 5.4.2.1A   | Outgoing subscriptions to load-control event .....  | 202 |
| 5.4.2.2    | Other subscriptions.....  | 202 |
| 5.4.3      | General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF ..... | 202 |
| 5.4.3.1    | Determination of UE-originated or UE-terminated case.....   | 202 |
| 5.4.3.2    | Requests initiated by the served user .....   | 203 |
| 5.4.3.3    | Requests terminated at the served user.....   | 212 |
| 5.4.3.4    | Original dialog identifier .....  | 221 |
| 5.4.3.5    | Void.....   | 221 |
| 5.4.3.6    | SIP digest authentication procedures for all SIP request methods initiated by the UE excluding REGISTER.....    | 221 |
| 5.4.3.6.1  | General .....   | 221 |
| 5.4.3.6.2  | Abnormal cases .....  | 223 |
| 5.4.4      | Call initiation .....   | 223 |
| 5.4.4.1    | Initial INVITE.....   | 223 |
| 5.4.4.2    | Subsequent requests .....   | 224 |
| 5.4.4.2.1  | UE-originating case .....   | 224 |



|            |  |     |
|------------|--|-----|
| 5.4.4.2.2  | UE-terminating case .....  | 224 |
| 5.4.5      | Call release.....  | 224 |
| 5.4.5.1    | S-CSCF-initiated session release .....   | 224 |
| 5.4.5.1.1  | Cancellation of a session currently being established.....                     | 224 |
| 5.4.5.1.2  | Release of an existing session .....   | 225 |
| 5.4.5.1.2A | Release of the existing dialogs due to registration expiration .....           | 226 |
| 5.4.5.1.3  | Abnormal cases .....   | 227 |
| 5.4.5.2    | Session release initiated by any other entity.....                             | 227 |
| 5.4.5.3    | Session expiration .....   | 227 |
| 5.4.6      | Call-related requests .....  | 227 |
| 5.4.6.1    | ReINVITE.....  | 227 |
| 5.4.6.1.1  | Determination of served user.....  | 227 |
| 5.4.6.1.2  | UE-originating case.....   | 227 |
| 5.4.6.1.3  | UE-terminating case .....  | 227 |
| 5.4.7      | Void .....   | 227 |
| 5.4.7A     | GRUU management.....   | 227 |
| 5.4.7A.1   | Overview of GRUU operation .....   | 227 |
| 5.4.7A.2   | Representation of public GRUUs.....  | 228 |
| 5.4.7A.3   | Representation of temporary GRUUs .....  | 229 |
| 5.4.7A.4   | GRUU recognition and validity .....  | 229 |
| 5.4.8      | Emergency service.....   | 230 |
| 5.4.8.1    | General .....  | 230 |
| 5.4.8.2    | Initial emergency registration or user-initiated emergency reregistration..... | 230 |
| 5.4.8.3    | User-initiated emergency deregistration .....                                  | 231 |
| 5.4.8.4    | Network-initiated emergency deregistration .....                               | 231 |
| 5.4.8.5    | Network-initiated emergency reauthentication .....                             | 231 |
| 5.4.8.6    | Subscription to the event providing registration state .....                   | 231 |
| 5.4.8.7    | Notification of the registration state.....                                    | 231 |
| 5.5        | Procedures at the MGCF .....   | 231 |
| 5.5.1      | General.....   | 231 |
| 5.5.2      | Subscription and notification .....  | 232 |
| 5.5.3      | Call initiation .....  | 232 |
| 5.5.3.1    | Initial INVITE.....  | 232 |
| 5.5.3.1.1  | Calls originated from circuit-switched networks.....                           | 232 |
| 5.5.3.1.2  | Calls terminating in circuit-switched networks .....                           | 233 |
| 5.5.3.2    | Subsequent requests .....  | 234 |
| 5.5.3.2.1  | Calls originating in circuit-switched networks .....                           | 234 |
| 5.5.3.2.2  | Calls terminating in circuit-switched networks .....                           | 234 |
| 5.5.4      | Call release.....  | 234 |
| 5.5.4.1    | Call release initiated by a circuit-switched network.....                      | 234 |
| 5.5.4.2    | IM CN subsystem initiated call release.....                                    | 234 |
| 5.5.4.3    | MGW-initiated call release .....   | 234 |
| 5.5.5      | Call-related requests .....  | 235 |
| 5.5.5.1    | ReINVITE.....  | 235 |
| 5.5.5.1.1  | Calls originating from circuit-switched networks .....                         | 235 |
| 5.5.5.1.2  | Calls terminating in circuit-switched networks .....                           | 235 |
| 5.5.6      | Further initial requests .....   | 235 |
| 5.6        | Procedures at the BGCF .....   | 235 |
| 5.6.1      | General.....   | 235 |
| 5.6.2      | Common BGCF procedures.....  | 235 |
| 5.6.3      | Specific procedures for INVITE requests and responses.....                     | 237 |
| 5.7        | Procedures at the Application Server (AS).....                                 | 238 |
| 5.7.1      | Common Application Server (AS) procedures .....                                | 238 |
| 5.7.1.1    | Notification about registration status .....                                   | 238 |
| 5.7.1.2    | Extracting charging correlation information .....                              | 239 |
| 5.7.1.3    | Access-Network-Info and Visited-Network-ID .....                               | 239 |
| 5.7.1.3A   | Determination of the served user .....   | 239 |
| 5.7.1.3A.1 | General .....  | 239 |
| 5.7.1.3A.2 | AS serving an originating user .....   | 239 |
| 5.7.1.3A.3 | AS serving a terminating user .....  | 240 |
| 5.7.1.4    | User identify verification at the AS.....                                      | 240 |
| 5.7.1.5    | Request authorization.....   | 242 |

|             |  |     |
|-------------|--|-----|
| 5.7.1.6     | Event notification throttling .....  | 242 |
| 5.7.1.7     | Local numbering .....  | 242 |
| 5.7.1.7.1   | Interpretation of the numbers in a non-international format .....            | 242 |
| 5.7.1.7.2   | Translation of the numbers in a non-international format .....               | 243 |
| 5.7.1.8     | GRUU assignment and usage .....  | 243 |
| 5.7.1.9     | Use of ICSI and IARI values .....  | 244 |
| 5.7.1.10    | Carrier selection .....  | 245 |
| 5.7.1.11    | Void .....   | 246 |
| 5.7.1.12    | Delivery of original destination identity .....                              | 246 |
| 5.7.1.13    | CPC and OLI .....  | 246 |
| 5.7.1.14    | Emergency transactions .....   | 246 |
| 5.7.1.15    | Protecting against attacks using 3xx responses .....                         | 247 |
| 5.7.1.16    | Support of Roaming Architecture for Voice over IMS with Local Breakout ..... | 247 |
| 5.7.1.16.1  | Preservation of parameters .....   | 247 |
| 5.7.1.16.2  | Preference for loopback routing not to occur .....                           | 247 |
| 5.7.1.17    | Delivery of network provided location information .....                      | 247 |
| 5.7.1.18    | Delivery of MRB address information .....                                    | 248 |
| 5.7.1.19    | Overload control .....   | 248 |
| 5.7.1.19.1  | Outgoing subscriptions to load-control event .....                           | 248 |
| 5.7.1.19.2  | Incoming subscriptions to load-control event .....                           | 248 |
| 5.7.2       | Application Server (AS) acting as terminating UA, or redirect server .....   | 248 |
| 5.7.3       | Application Server (AS) acting as originating UA .....                       | 249 |
| 5.7.4       | Application Server (AS) acting as a SIP proxy .....                          | 251 |
| 5.7.5       | Application Server (AS) performing 3rd party call control .....              | 251 |
| 5.7.5.1     | General .....  | 251 |
| 5.7.5.2     | Call initiation .....  | 253 |
| 5.7.5.2.1   | Initial INVITE .....   | 253 |
| 5.7.5.2.2   | Subsequent requests .....  | 253 |
| 5.7.5.3     | Call release .....   | 253 |
| 5.7.5.4     | Call-related requests .....  | 253 |
| 5.7.5.5     | Further initial requests .....   | 254 |
| 5.7.5.6     | Transcoding services invocation using third-party call control .....         | 254 |
| 5.7.6       | Void .....   | 254 |
| 5.8         | Procedures at the MRFC .....   | 254 |
| 5.8.1       | General .....  | 254 |
| 5.8.2       | Call initiation .....  | 255 |
| 5.8.2.1     | Initial INVITE .....   | 255 |
| 5.8.2.1.1   | MRFC-terminating case .....  | 255 |
| 5.8.2.1.1.1 | Introduction .....   | 255 |
| 5.8.2.1.2   | MRFC-originating case .....  | 255 |
| 5.8.2.2     | Subsequent requests .....  | 256 |
| 5.8.2.2.1   | Tones and announcements .....  | 256 |
| 5.8.2.2.2   | Transcoding .....  | 256 |
| 5.8.3       | Call release .....   | 256 |
| 5.8.3.1     | S-CSCF-initiated call release .....  | 256 |
| 5.8.3.1.1   | Tones and announcements .....  | 256 |
| 5.8.3.2     | MRFC-initiated call release .....  | 256 |
| 5.8.3.2.1   | Tones and announcements .....  | 256 |
| 5.8.4       | Call-related requests .....  | 256 |
| 5.8.4.1     | ReINVITE .....   | 256 |
| 5.8.4.1.1   | MRFC-terminating case .....  | 256 |
| 5.8.4.1.2   | MRFC-originating case .....  | 256 |
| 5.8.4.2     | REFER .....  | 256 |
| 5.8.4.2.1   | MRFC-terminating case .....  | 256 |
| 5.8.4.2.2   | MRFC-originating case .....  | 256 |
| 5.8.4.2.3   | REFER initiating a new session .....   | 257 |
| 5.8.4.2.4   | REFER replacing an existing session .....                                    | 257 |
| 5.8.4.3     | INFO .....   | 257 |
| 5.8.5       | Further initial requests .....   | 257 |
| 5.8A        | Procedures at the MRB .....  | 257 |
| 5.9         | Void .....   | 257 |
| 5.9.1       | Void .....   | 257 |

|           |   |     |
|-----------|---|-----|
| 5.10      | Procedures at the IBCF.....   | 257 |
| 5.10.1    | General.....  | 257 |
| 5.10.2    | IBCF as an exit point .....   | 258 |
| 5.10.2.1  | Registration .....  | 258 |
| 5.10.2.1A | General .....   | 258 |
| 5.10.2.2  | Initial requests .....  | 259 |
| 5.10.2.3  | Subsequent requests .....   | 260 |
| 5.10.2.4  | IBCF-initiated call release.....  | 260 |
| 5.10.3    | IBCF as an entry point.....   | 260 |
| 5.10.3.1  | Registration .....  | 260 |
| 5.10.3.1A | General .....   | 261 |
| 5.10.3.2  | Initial requests .....  | 261 |
| 5.10.3.3  | Subsequent requests .....   | 263 |
| 5.10.3.4  | IBCF-initiated call release.....  | 263 |
| 5.10.3.5  | Abnormal cases .....  | 264 |
| 5.10.4    | THING functionality in the IBCF.....  | 264 |
| 5.10.4.1  | General .....   | 264 |
| 5.10.4.2  | Encryption for network topology hiding .....                                      | 265 |
| 5.10.4.3  | Decryption for network topology hiding.....                                       | 266 |
| 5.10.5    | IMS-ALG functionality in the IBCF.....  | 266 |
| 5.10.6    | Screening of SIP signalling.....  | 267 |
| 5.10.6.1  | General .....   | 267 |
| 5.10.6.2  | IBCF procedures for SIP header fields.....  | 267 |
| 5.10.6.3  | IBCF procedures for SIP message bodies .....                                      | 268 |
| 5.10.7    | Media transcoding control .....   | 268 |
| 5.10.7.1  | General .....   | 268 |
| 5.10.7.2  | Media transcoding control procedures .....  | 268 |
| 5.10.8    | Privacy protection at the trust domain boundary .....                             | 269 |
| 5.10.9    | Roaming architecture for voice over IMS with local breakout .....                 | 270 |
| 5.11      | Procedures at the E-CSCF .....  | 270 |
| 5.11.1    | General.....  | 270 |
| 5.11.2    | UE originating case.....  | 270 |
| 5.11.3    | Use of an LRF.....  | 273 |
| 5.11.4    | Subscriptions to E-CSCF events .....  | 275 |
| 5.11.4.1  | Subscription to the event providing dialog state .....                            | 275 |
| 5.11.4.2  | Notification about dialog state .....   | 275 |
| 5.12      | Location Retrieval Function (LRF) .....   | 276 |
| 5.12.1    | General.....  | 276 |
| 5.12.2    | Treatment of incoming initial requests for a dialog and standalone requests ..... | 276 |
| 5.12.3    | Subscription and notification .....   | 277 |
| 5.12.3.1  | Notification about dialog state .....   | 277 |
| 5.13      | ISC gateway function .....  | 278 |
| 5.13.1    | General.....  | 278 |
| 5.13.2    | ISC gateway function as an exit point .....                                       | 279 |
| 5.13.2.1  | Registration .....  | 279 |
| 5.13.2.2  | General .....   | 279 |
| 5.13.2.3  | Initial requests .....  | 279 |
| 5.13.2.4  | Subsequent requests .....   | 280 |
| 5.13.2.5  | Call release initiated by ISC gateway function .....                              | 281 |
| 5.13.3    | ISC gateway function as an entry point .....                                      | 281 |
| 5.13.3.1  | Registration .....  | 281 |
| 5.13.3.2  | General .....   | 281 |
| 5.13.3.3  | Initial requests .....  | 281 |
| 5.13.3.4  | Subsequent requests .....   | 282 |
| 5.13.3.5  | Call release initiated by the ISC gateway function .....                          | 283 |
| 5.13.4    | THING functionality in the ISC gateway function.....                              | 283 |
| 5.13.5    | IMS-ALG functionality in the ISC gateway function.....                            | 283 |
| 5.13.6    | Screening of SIP signalling.....  | 283 |
| 6         | Application usage of SDP .....  | 284 |
| 6.1       | Procedures at the UE .....  | 284 |
| 6.1.1     | General.....  | 284 |

|             |   |     |
|-------------|---|-----|
| 6.1.2       | Handling of SDP at the originating UE .....                               | 285 |
| 6.1.3       | Handling of SDP at the terminating UE.....                                | 286 |
| 6.2         | Procedures at the P-CSCF .....  | 287 |
| 6.3         | Procedures at the S-CSCF .....  | 289 |
| 6.4         | Procedures at the MGCF .....  | 289 |
| 6.4.1       | Calls originating from circuit-switched networks.....                     | 289 |
| 6.4.2       | Calls terminating in circuit-switched networks.....                       | 289 |
| 6.4.3       | Optimal Media Routeing (OMR).....   | 290 |
| 6.4.4       | Explicit congestion control support in MGCF.....                          | 290 |
| 6.5         | Procedures at the MRFC .....  | 290 |
| 6.6         | Procedures at the AS .....  | 290 |
| 6.7         | Procedures at the IMS-ALG functionality.....                              | 291 |
| 6.7.1       | IMS-ALG in IBCF.....  | 291 |
| 6.7.1.1     | General .....   | 291 |
| 6.7.1.2     | IMS-ALG in IBCF for support of ICE.....                                   | 291 |
| 6.7.1.2.1   | General .....   | 291 |
| 6.7.1.2.2   | IBCF full ICE procedures for UDP based streams .....                      | 291 |
| 6.7.1.2.2.1 | General.....  | 291 |
| 6.7.1.2.2.2 | IBCF receiving SDP offer.....   | 291 |
| 6.7.1.2.2.3 | IBCF sending SDP offer .....  | 292 |
| 6.7.1.2.2.4 | IBCF receiving SDP answer .....   | 292 |
| 6.7.1.2.2.5 | IBCF sending SDP answer.....  | 292 |
| 6.7.1.2.3   | IBCF ICE lite procedures for UDP based streams .....                      | 292 |
| 6.7.1.2.4   | ICE procedures for TCP based streams .....                                | 293 |
| 6.7.1.2.4.1 | General.....  | 293 |
| 6.7.1.2.4.2 | IBCF receiving SDP offer.....   | 293 |
| 6.7.1.2.4.3 | IBCF sending SDP offer .....  | 293 |
| 6.7.1.2.4.4 | IBCF receiving SDP answer .....   | 293 |
| 6.7.1.2.4.5 | IBCF sending SDP answer.....  | 293 |
| 6.7.2       | IMS-ALG in P-CSCF .....   | 293 |
| 6.7.2.1     | General .....   | 293 |
| 6.7.2.2     | IMS-ALG in P-CSCF for media plane security .....                          | 294 |
| 6.7.2.3     | IMS-ALG in P-CSCF for explicit congestion control support.....            | 294 |
| 6.7.2.3.1   | General .....   | 294 |
| 6.7.2.3.2   | Incoming SDP offer with ECN.....  | 294 |
| 6.7.2.3.3   | Incoming SDP offer without ECN.....                                       | 295 |
| 6.7.2.4     | IMS-ALG in P-CSCF for Optimal Media Routeing (OMR).....                   | 295 |
| 6.7.2.5     | IMS-ALG in P-CSCF for NA(P)T and NA(P)T-PT controlled by the P-CSCF ..... | 295 |
| 6.7.2.5.1   | General .....   | 295 |
| 6.7.2.6     | IMS-ALG in P-CSCF for support of hosted NAT .....                         | 296 |
| 6.7.2.6.1   | General .....   | 296 |
| 6.7.2.7     | IMS-ALG in P-CSCF for support of ICE .....                                | 296 |
| 6.7.2.7.1   | General .....   | 296 |
| 6.7.2.7.2   | P-CSCF full ICE procedures for UDP based streams.....                     | 296 |
| 6.7.2.7.2.1 | General.....  | 296 |
| 6.7.2.7.2.2 | P-CSCF receiving SDP offer .....  | 296 |
| 6.7.2.7.2.3 | P-CSCF sending SDP offer.....   | 297 |
| 6.7.2.7.2.4 | P-CSCF receiving SDP answer.....  | 297 |
| 6.7.2.7.2.5 | P-CSCF sending SDP answer .....   | 297 |
| 6.7.2.7.3   | P-CSCF ICE lite procedures for UDP based streams .....                    | 297 |
| 6.7.2.7.4   | ICE procedures for TCP based streams .....                                | 297 |
| 6.7.2.7.4.1 | General.....  | 297 |
| 6.7.2.7.4.2 | P-CSCF receiving SDP offer .....  | 298 |
| 6.7.2.7.4.3 | P-CSCF sending SDP offer.....   | 298 |
| 6.7.2.7.4.4 | P-CSCF receiving SDP answer.....  | 298 |
| 6.7.2.7.4.5 | P-CSCF sending SDP answer .....   | 298 |
| 6.7.2.8     | IMS-ALG in P-CSCF for transcoding.....                                    | 298 |
| 6.7.3       | IMS-ALG in ISC gateway function.....                                      | 299 |
| 6.7.3.1     | General .....   | 299 |
| 6.7.3.2     | IMS-ALG in application gateway function for support of ICE.....           | 299 |
| 7           | Extensions within the present document .....                              | 299 |

|            |  |     |
|------------|--|-----|
| 7.1        | SIP methods defined within the present document.....                                 | 299 |
| 7.2        | SIP header fields defined within the present document.....                           | 299 |
| 7.2.0      | General.....   | 299 |
| 7.2.1      | Void.....  | 300 |
| 7.2.2      | Void.....  | 300 |
| 7.2.3      | Void.....  | 300 |
| 7.2.4      | Void.....  | 300 |
| 7.2.5      | Void.....  | 300 |
| 7.2.6      | Void.....  | 300 |
| 7.2.7      | Void.....  | 300 |
| 7.2.8      | Void.....  | 300 |
| 7.2.9      | Void.....  | 300 |
| 7.2.10     | Void.....  | 300 |
| 7.2A       | Extensions to SIP header fields defined within the present document.....             | 300 |
| 7.2A.1     | Extension to WWW-Authenticate header field.....                                      | 300 |
| 7.2A.1.1   | Introduction.....  | 300 |
| 7.2A.1.2   | Syntax.....  | 300 |
| 7.2A.1.3   | Operation.....   | 300 |
| 7.2A.2     | Extension to Authorization header field.....   | 300 |
| 7.2A.2.1   | Introduction.....  | 300 |
| 7.2A.2.2   | Syntax.....  | 301 |
| 7.2A.2.3   | Operation.....   | 301 |
| 7.2A.3     | Tokenized-by header field parameter definition (various header fields).....          | 302 |
| 7.2A.3.1   | Introduction.....  | 302 |
| 7.2A.3.2   | Syntax.....  | 302 |
| 7.2A.3.3   | Operation.....   | 302 |
| 7.2A.4     | P-Access-Network-Info header field.....  | 302 |
| 7.2A.4.1   | Introduction.....  | 302 |
| 7.2A.4.2   | Syntax.....  | 302 |
| 7.2A.4.3   | Additional coding rules for P-Access-Network-Info header field.....                  | 303 |
| 7.2A.5     | P-Charging-Vector header field.....  | 305 |
| 7.2A.5.1   | Introduction.....  | 305 |
| 7.2A.5.2   | Syntax.....  | 305 |
| 7.2A.5.2.1 | General.....   | 305 |
| 7.2A.5.2.2 | GPRS as IP-CAN.....  | 307 |
| 7.2A.5.2.3 | I-WLAN as IP-CAN.....  | 307 |
| 7.2A.5.2.4 | xDSL as IP-CAN.....  | 307 |
| 7.2A.5.2.5 | DOCSIS as IP-CAN.....  | 308 |
| 7.2A.5.2.6 | cdma2000 <sup>®</sup> packet data subsystem as IP-CAN.....                           | 308 |
| 7.2A.5.2.7 | EPS as IP-CAN.....   | 308 |
| 7.2A.5.2.8 | Ethernet as IP-CAN.....  | 309 |
| 7.2A.5.2.9 | Fiber as IP-CAN.....   | 309 |
| 7.2A.5.3   | Operation.....   | 309 |
| 7.2A.6     | Orig parameter definition.....   | 309 |
| 7.2A.6.1   | Introduction.....  | 309 |
| 7.2A.6.2   | Syntax.....  | 309 |
| 7.2A.6.3   | Operation.....   | 309 |
| 7.2A.7     | Extension to Security-Client, Security-Server and Security-Verify header fields..... | 309 |
| 7.2A.7.1   | Introduction.....  | 309 |
| 7.2A.7.2   | Syntax.....  | 310 |
| 7.2A.7.2.1 | General.....   | 310 |
| 7.2A.7.2.2 | "mediasec" header field parameter.....   | 310 |
| 7.2A.7.3   | Operation.....   | 310 |
| 7.2A.7.4   | IANA registration.....   | 311 |
| 7.2A.7.4.1 | "mediasec" header field parameter.....   | 311 |
| 7.2A.7.4.2 | "sdes-srtp" security mechanism.....  | 311 |
| 7.2A.8     | IMS Communication Service Identifier (ICSI).....                                     | 312 |
| 7.2A.8.1   | Introduction.....  | 312 |
| 7.2A.8.2   | Coding of the ICSI.....  | 312 |
| 7.2A.9     | IMS Application Reference Identifier (IARI).....                                     | 312 |
| 7.2A.9.1   | Introduction.....  | 312 |
| 7.2A.9.2   | Coding of the IARI.....  | 312 |

|           |  |     |
|-----------|--|-----|
| 7.2A.10   | "phone-context" tel URI parameter.....                             | 313 |
| 7.2A.10.1 | Introduction.....  | 313 |
| 7.2A.10.2 | Syntax .....   | 313 |
| 7.2A.10.3 | Additional coding rules for "phone-context" tel URI parameter..... | 313 |
| 7.2A.11   | Void.....  | 314 |
| 7.2A.11.1 | Void.....  | 314 |
| 7.2A.11.2 | Void.....  | 314 |
| 7.2A.11.3 | Void.....  | 314 |
| 7.2A.12   | CPC and OLI tel URI parameter definition .....                     | 314 |
| 7.2A.12.1 | Introduction.....  | 314 |
| 7.2A.12.2 | Syntax .....   | 314 |
| 7.2A.12.3 | Operation.....   | 315 |
| 7.2A.13   | "sos" SIP URI parameter .....                                      | 315 |
| 7.2A.13.1 | Introduction.....  | 315 |
| 7.2A.13.2 | Syntax .....   | 315 |
| 7.2A.13.3 | Operation.....   | 315 |
| 7.2A.14   | P-Associated-URI header field .....                                | 315 |
| 7.2A.15   | Void .....   | 316 |
| 7.2A.16   | Extension to History-Info header field.....                        | 316 |
| 7.2A.16.1 | Introduction.....  | 316 |
| 7.2A.16.2 | Syntax .....   | 316 |
| 7.2A.16.3 | Operation.....   | 316 |
| 7.3       | Option-tags defined within the present document .....              | 316 |
| 7.4       | Status-codes defined within the present document.....              | 316 |
| 7.5       | Session description types defined within the present document..... | 316 |
| 7.5.1     | General.....   | 316 |
| 7.5.2     | End-to-access-edge media plane security .....                      | 317 |
| 7.5.2.1   | General .....  | 317 |
| 7.5.2.2   | Syntax .....   | 317 |
| 7.5.2.3   | IANA registration .....  | 317 |
| 7.5.3     | Optimal Media Routeing (OMR) attributes.....                       | 318 |
| 7.5.3.1   | General .....  | 318 |
| 7.5.3.2   | Semantics .....  | 318 |
| 7.5.3.3   | Syntax .....   | 318 |
| 7.5.3.4   | IANA registration .....  | 320 |
| 7.5.3.4.1 | visited-realm attribute.....                                       | 320 |
| 7.5.3.4.2 | secondary-realm attribute .....                                    | 321 |
| 7.5.3.4.3 | omr-s-cksum attribute.....   | 321 |
| 7.5.3.4.4 | omr-m-cksum attribute .....  | 321 |
| 7.5.3.4.5 | omr-codecs attribute .....   | 321 |
| 7.5.3.4.6 | omr-m-att attribute.....   | 322 |
| 7.5.3.4.7 | omr-s-att attribute .....  | 322 |
| 7.5.3.4.8 | omr-m-bw attribute.....  | 322 |
| 7.5.3.4.9 | omr-s-bw attribute .....   | 323 |
| 7.6       | 3GPP IM CN subsystem XML body.....                                 | 323 |
| 7.6.1     | General.....   | 323 |
| 7.6.2     | Document Type Definition .....                                     | 323 |
| 7.6.3     | XML Schema description .....                                       | 324 |
| 7.6.4     | MIME type definition .....   | 325 |
| 7.6.4.1   | Introduction.....  | 325 |
| 7.6.4.2   | Syntax .....   | 325 |
| 7.6.4.3   | Operation.....   | 325 |
| 7.6.5     | IANA Registration.....   | 326 |
| 7.7       | SIP timers .....   | 327 |
| 7.8       | IM CN subsystem timers.....  | 328 |
| 7.9       | Media feature tags defined within the current document .....       | 328 |
| 7.9.1     | General.....   | 328 |
| 7.9.2     | Definition of media feature tag g.3gpp.icsi-ref.....               | 329 |
| 7.9.3     | Definition of media feature tag g.3gpp.iari-ref .....              | 329 |
| 7.9.4     | Void .....   | 330 |
| 7.9.5     | Void .....   | 330 |
| 7.9.6     | Void .....   | 330 |

|             |   |     |
|-------------|---|-----|
| 7.9A        | Feature-capability indicators defined within the current document .....           | 330 |
| 7.9A.1      | General.....  | 330 |
| 7.9A.2      | Definition of feature-capability indicator g.3gpp.icsi-ref .....                  | 330 |
| 7.9A.3      | Definition of feature-capability indicators g.3gpp.trf .....                      | 330 |
| 7.9A.4      | Definition of feature-capability indicator g.3gpp.loopback .....                  | 331 |
| 7.9A.5      | Definition of feature-capability indicator g.3gpp.home-visited.....               | 331 |
| 7.9A.6      | Definition of feature-capability indicator g.3gpp.mrb .....                       | 332 |
| 7.10        | Reg-event package extensions defined within the current document.....             | 333 |
| 7.10.1      | General.....  | 333 |
| 7.10.2      | Reg-Event package extension to transport wildcarded public user identities .....  | 333 |
| 7.10.2.1    | Structure and data semantics .....  | 333 |
| 7.10.2.2    | XML Schema .....  | 333 |
| 7.10.3      | Reg-event package extension for policy transport.....                             | 333 |
| 7.10.3.1    | Scope.....  | 333 |
| 7.10.3.2    | Structure and data semantics .....  | 333 |
| 7.10.3.3    | XML Schema .....  | 334 |
| 7.11        | Void.....   | 335 |
| 7.12        | Info package definitions and associated MIME type definitions.....                | 335 |
| 7.12.1      | DTMF info package and session-info MIME type .....                                | 335 |
| 7.12.1.1    | DTMF info package .....   | 335 |
| 7.12.1.1.1  | General .....   | 335 |
| 7.12.1.1.2  | Overall description .....   | 335 |
| 7.12.1.1.3  | Applicability .....   | 336 |
| 7.12.1.1.4  | Info package name.....  | 336 |
| 7.12.1.1.5  | Info package parameters .....   | 336 |
| 7.12.1.1.6  | SIP option tags.....  | 336 |
| 7.12.1.1.7  | INFO message body parts.....  | 336 |
| 7.12.1.1.8  | Info package usage restrictions.....  | 336 |
| 7.12.1.1.9  | Rate of INFO requests .....   | 336 |
| 7.12.1.1.10 | Info package security considerations.....   | 336 |
| 7.12.1.2    | Overlap digit message body .....  | 336 |
| 7.12.1.2.1  | Scope .....   | 336 |
| 7.12.1.2.2  | MIME type .....   | 337 |
| 7.12.1.2.3  | ABNF .....  | 337 |
| 7.12.1.2.4  | IANA registration template .....  | 337 |
| 7.12.1.3    | Implementation details and examples .....   | 338 |
| 8           | SIP compression.....  | 338 |
| 8.1         | SIP compression procedures at the UE.....   | 338 |
| 8.1.1       | SIP compression .....   | 338 |
| 8.1.2       | Compression of SIP requests and responses transmitted to the P-CSCF .....         | 339 |
| 8.1.3       | Decompression of SIP requests and responses received from the P-CSCF .....        | 339 |
| 8.2         | SIP compression procedures at the P-CSCF.....                                     | 339 |
| 8.2.1       | SIP compression .....   | 339 |
| 8.2.2       | Compression of SIP requests and responses transmitted to the UE .....             | 340 |
| 8.2.3       | Decompression of SIP requests and responses received from the UE .....            | 340 |
| 9           | IP-Connectivity Access Network aspects when connected to the IM CN subsystem..... | 340 |
| 9.1         | Introduction .....  | 340 |
| 9.2         | Procedures at the UE .....  | 340 |
| 9.2.1       | Connecting to the IP-CAN and P-CSCF discovery .....                               | 340 |
| 9.2.2       | Handling of the IP-CAN .....  | 341 |
| 9.2.2A      | P-CSCF restoration procedure .....  | 341 |
| 9.2.3       | Special requirements applying to forked responses .....                           | 341 |
| 10          | Media control .....   | 342 |
| 10.1        | General .....   | 342 |
| 10.2        | Procedures at the AS .....  | 342 |
| 10.2.1      | General.....  | 342 |
| 10.2.2      | Tones and announcements .....   | 342 |
| 10.2.2.1    | General .....   | 342 |
| 10.2.2.2    | Basic network media services with SIP .....                                       | 343 |
| 10.2.2.3    | SIP interface to VoiceXML media services .....                                    | 343 |

|  |  |            |
|--|--|------------|
| 10.2.2.4   | Media control channel framework and packages .....   | 343        |
| 10.2.3   | Ad-hoc conferences .....   | 343        |
| 10.2.3.1   | General .....  | 343        |
| 10.2.3.2   | Basic network media services with SIP .....  | 343        |
| 10.2.3.3   | Media control channel framework and packages .....   | 343        |
| 10.2.4   | Transcoding .....  | 344        |
| 10.2.4.1   | General .....  | 344        |
| 10.2.4.2   | Basic network media services with SIP .....  | 344        |
| 10.2.4.3   | Media control channel framework and packages .....   | 344        |
| 10.3   | Procedures at the MRFC .....   | 344        |
| 10.3.1   | General .....  | 344        |
| 10.3.2   | Tones and announcements .....  | 344        |
| 10.3.2.1   | General .....  | 344        |
| 10.3.2.2   | Basic network media services with SIP .....  | 345        |
| 10.3.2.3   | SIP interface to VoiceXML media services .....   | 345        |
| 10.3.2.4   | Media control channel framework and packages .....   | 345        |
| 10.3.3   | Ad-hoc conferences .....   | 345        |
| 10.3.3.1   | General .....  | 345        |
| 10.3.3.2   | Basic network media services with SIP .....  | 345        |
| 10.3.3.3   | Media control channel framework and packages .....   | 345        |
| 10.3.4   | Transcoding .....  | 346        |
| 10.3.4.1   | General .....  | 346        |
| 10.3.4.2   | Basic network media services with SIP .....  | 346        |
| 10.3.4.3   | Media control channel framework and packages .....   | 346        |
| 10.4   | Procedures at the MRB .....  | 346        |
| <b>Annex A (normative): Profiles of IETF RFCs for 3GPP usage .....</b> |  | <b>347</b> |
| A.1  | Profiles .....   | 347        |
| A.1.1  | Relationship to other specifications .....   | 347        |
| A.1.2  | Introduction to methodology within this profile .....  | 347        |
| A.1.3  | Roles .....  | 349        |
| A.2  | Profile definition for the Session Initiation Protocol as used in the present document ..... | 355        |
| A.2.1  | User agent role .....  | 355        |
| A.2.1.1  | Introduction .....   | 355        |
| A.2.1.2  | Major capabilities .....   | 356        |
| A.2.1.3  | PDU's .....  | 369        |
| A.2.1.4  | PDU parameters .....   | 370        |
| A.2.1.4.1  | Status-codes .....   | 370        |
| A.2.1.4.2  | ACK method .....   | 374        |
| A.2.1.4.3  | BYE method .....   | 377        |
| A.2.1.4.4  | CANCEL method .....  | 385        |
| A.2.1.4.5  | COMET method .....   | 388        |
| A.2.1.4.6  | INFO method .....  | 388        |
| A.2.1.4.7  | INVITE method .....  | 396        |
| A.2.1.4.7A   | MESSAGE method .....   | 412        |
| A.2.1.4.8  | NOTIFY method .....  | 421        |
| A.2.1.4.9  | OPTIONS method .....   | 430        |
| A.2.1.4.10   | PRACK method .....   | 438        |
| A.2.1.4.10A  | PUBLISH method .....   | 445        |
| A.2.1.4.11   | REFER method .....   | 454        |
| A.2.1.4.12   | REGISTER method .....  | 463        |
| A.2.1.4.13   | SUBSCRIBE method .....   | 472        |
| A.2.1.4.14   | UPDATE method .....  | 481        |
| A.2.2  | Proxy role .....   | 489        |
| A.2.2.1  | Introduction .....   | 489        |
| A.2.2.2  | Major capabilities .....   | 490        |
| A.2.2.3  | PDU's .....  | 500        |
| A.2.2.4  | PDU parameters .....   | 501        |
| A.2.2.4.1  | Status-codes .....   | 501        |
| A.2.2.4.2  | ACK method .....   | 505        |
| A.2.2.4.3  | BYE method .....   | 508        |



|                             |  |            |
|-----------------------------|--|------------|
| A.2.2.4.4                   | CANCEL method.....   | 518        |
| A.2.2.4.5                   | COMET method.....  | 521        |
| A.2.2.4.6                   | INFO method .....  | 521        |
| A.2.2.4.7                   | INVITE method .....  | 529        |
| A.2.2.4.7A                  | MESSAGE method .....   | 545        |
| A.2.2.4.8                   | NOTIFY method .....  | 555        |
| A.2.2.4.9                   | OPTIONS method.....  | 565        |
| A.2.2.4.10                  | PRACK method .....   | 574        |
| A.2.2.4.10A                 | PUBLISH method.....  | 582        |
| A.2.2.4.11                  | REFER method .....   | 592        |
| A.2.2.4.12                  | REGISTER method.....   | 602        |
| A.2.2.4.13                  | SUBSCRIBE method.....  | 611        |
| A.2.2.4.14                  | UPDATE method.....   | 622        |
| A.3                         | Profile definition for the Session Description Protocol as used in the present document.....   | 631        |
| A.3.1                       | Introduction .....   | 631        |
| A.3.2                       | User agent role .....  | 631        |
| A.3.2.1                     | Major capabilities .....   | 632        |
| A.3.2.2                     | SDP types .....  | 635        |
| A.3.2.3                     | Void .....   | 641        |
| A.3.2.4                     | Void .....   | 641        |
| A.3.3                       | Proxy role .....   | 641        |
| A.3.3.1                     | Major capabilities .....   | 642        |
| A.3.3.2                     | SDP types .....  | 643        |
| A.3.3.3                     | Void .....   | 649        |
| A.3.3.4                     | Void .....   | 649        |
| A.4                         | Profile definition for other message bodies as used in the present document.....   | 649        |
| <b>Annex B (normative):</b> | <b>IP-Connectivity Access Network specific concepts when using GPRS to access IM CN subsystem.....</b>   | <b>650</b> |
| B.1                         | Scope .....  | 650        |
| B.2                         | GPRS aspects when connected to the IM CN subsystem.....  | 650        |
| B.2.1                       | Introduction .....   | 650        |
| B.2.2                       | Procedures at the UE .....   | 650        |
| B.2.2.1                     | PDP context activation and P-CSCF discovery .....  | 650        |
| B.2.2.1A                    | Modification of a PDP context used for SIP signalling .....  | 652        |
| B.2.2.1B                    | Re-establishment of the PDP context for SIP signalling.....  | 653        |
| B.2.2.1C                    | P-CSCF restoration procedure .....   | 653        |
| B.2.2.2                     | Session management procedures .....  | 654        |
| B.2.2.3                     | Mobility management procedures.....  | 654        |
| B.2.2.4                     | Cell selection and lack of coverage.....   | 654        |
| B.2.2.5                     | PDP contexts for media .....   | 654        |
| B.2.2.5.1                   | General requirements .....   | 654        |
| B.2.2.5.1A                  | Activation or modification of PDP contexts for media by the UE.....  | 654        |
| B.2.2.5.1B                  | Activation or modification of PDP contexts for media by the GGSN .....   | 655        |
| B.2.2.5.1C                  | Deactivation of PDP context for media.....   | 656        |
| B.2.2.5.2                   | Special requirements applying to forked responses .....  | 656        |
| B.2.2.5.3                   | Unsuccessful situations .....  | 656        |
| B.2.2.6                     | Emergency service.....   | 656        |
| B.2A                        | Usage of SDP .....   | 658        |
| B.2A.0                      | General .....  | 658        |
| B.2A.1                      | Impact on SDP offer / answer of activation or modification of PDP contexts for media by the network .....  | 658        |
| B.2A.2                      | Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE..... | 658        |
| B.2A.3                      | Emergency service .....  | 659        |
| B.3                         | Application usage of SIP .....   | 659        |
| B.3.1                       | Procedures at the UE .....   | 659        |
| B.3.1.1                     | P-Access-Network-Info header field .....   | 659        |
| B.3.1.2                     | Availability for calls .....   | 659        |

|   |  |            |
|---|--|------------|
| B.3.1.2A  | Availability for SMS.....  | 659        |
| B.3.1.3   | Authorization header field .....   | 659        |
| B.3.1.4   | SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE ..... | 660        |
| B.3.2   | Procedures at the P-CSCF .....   | 660        |
| B.3.2.1   | Determining network to which the originating user is attached.....   | 660        |
| B.3.2.2   | Location information handling .....  | 660        |
| B.3.2.3   | Prohibited usage of PDN connection for emergency bearer services .....   | 660        |
| B.3.3   | Procedures at the S-CSCF .....   | 660        |
| B.3.3.1   | Notification of AS about registration status.....  | 660        |
| B.4   | 3GPP specific encoding for SIP header field extensions .....   | 661        |
| B.4.1   | Void.....  | 661        |
| B.5   | Use of circuit-switched domain.....  | 661        |
| <b>Annex C (normative): UICC and USIM Aspects for access to the IM CN subsystem.....</b>                                      |  | <b>662</b> |
| C.1   | Scope .....  | 662        |
| C.2   | Derivation of IMS parameters from USIM .....   | 662        |
| C.3   | ISIM Location in 3GPP Systems.....   | 662        |
| C.3A  | UICC access to IMS .....   | 662        |
| C.4   | Update of IMS parameters on the UICC .....   | 663        |
| <b>Annex D (normative): IP-Connectivity Access Network specific concepts when using I-WLAN to access IM CN subsystem.....</b> |  | <b>664</b> |
| D.1   | Scope .....  | 664        |
| D.2   | I-WLAN aspects when connected to the IM CN subsystem .....   | 664        |
| D.2.1   | Introduction .....   | 664        |
| D.2.2   | Procedures at the WLAN UE .....  | 664        |
| D.2.2.1   | I-WLAN tunnel activation and P-CSCF discovery.....   | 664        |
| D.2.2.1A  | Modification of a I-WLAN tunnel used for SIP signalling .....  | 665        |
| D.2.2.1B  | Re-establishment of the I-WLAN tunnel used for SIP signalling.....   | 665        |
| D.2.2.1C  | P-CSCF restoration procedure .....   | 665        |
| D.2.2.2   | Void .....   | 665        |
| D.2.2.3   | Void .....   | 665        |
| D.2.2.4   | Void .....   | 665        |
| D.2.2.5   | I-WLAN tunnel procedures for media .....   | 665        |
| D.2.2.5.1   | General requirements .....   | 665        |
| D.2.2.5.1A  | Activation or modification of I-WLAN tunnel for media by the WLAN UE .....   | 666        |
| D.2.2.5.1B  | Activation or modification of I-WLAN tunnel for media by the network .....   | 666        |
| D.2.2.5.1C  | Deactivation of I-WLAN tunnel for media .....  | 666        |
| D.2.2.5.2   | Special requirements applying to forked responses .....  | 666        |
| D.2.2.5.3   | Unsuccessful situations .....  | 666        |
| D.2.2.6   | Emergency service.....   | 666        |
| D.2A  | Usage of SDP .....   | 666        |
| D.2A.0  | General .....  | 666        |
| D.2A.1  | Impact on SDP offer / answer of activation or modification of I-WLAN tunnel for media by the network ..  | 666        |
| D.2A.2  | Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE.....   | 667        |
| D.2A.3  | Emergency service .....  | 667        |
| D.3   | Application usage of SIP .....   | 667        |
| D.3.1   | Procedures at the UE .....   | 667        |
| D.3.1.1   | P-Access-Network-Info header field .....   | 667        |
| D.3.1.2   | Availability for calls .....   | 667        |
| D.3.1.2A  | Availability for SMS.....  | 667        |
| D.3.1.3   | Authorization header field .....   | 667        |

|         |  |     |
|---------|--|-----|
| D.3.1.4 | SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE ..... | 667 |
| D.3.2   | Procedures at the P-CSCF .....   | 667 |
| D.3.2.1 | Determining network to which the originating user is attached.....   | 667 |
| D.3.2.2 | Location information handling .....  | 667 |
| D.3.3   | Procedures at the S-CSCF .....   | 667 |
| D.3.3.1 | Notification of AS about registration status.....  | 667 |
| D.4     | 3GPP specific encoding for SIP header field extensions .....   | 668 |
| D.5     | Use of circuit-switched domain.....  | 668 |

**Annex E (normative): IP-Connectivity Access Network specific concepts when using xDSL, Fiber or Ethernet to access IM CN subsystem.....669**

|            |  |     |
|------------|--|-----|
| E.1        | Scope .....  | 669 |
| E.2        | Fixed broadband aspects when connected to the IM CN subsystem.....   | 669 |
| E.2.1      | Introduction .....   | 669 |
| E.2.2      | Procedures at the UE .....   | 669 |
| E.2.2.1    | Activation and P-CSCF discovery .....  | 669 |
| E.2.2.1A   | Modification of a fixed-broadband connection used for SIP signalling .....   | 670 |
| E.2.2.1B   | Re-establishment of a fixed-broadband connection used for SIP signalling.....  | 670 |
| E.2.2.1C   | P-CSCF restoration procedure .....   | 670 |
| E.2.2.2    | Void .....   | 670 |
| E.2.2.3    | Void .....   | 670 |
| E.2.2.4    | Void.....  | 670 |
| E.2.2.5    | Fixed-broadband bearer(s) for media.....   | 670 |
| E.2.2.5.1  | General requirements .....   | 670 |
| E.2.2.5.1A | Activation or modification of fixed-broadband bearers for media by the UE.....   | 670 |
| E.2.2.5.1B | Activation or modification of fixed-broadband bearers for media by the network .....   | 670 |
| E.2.2.5.1C | Deactivation of fixed-broadband bearers for media.....   | 670 |
| E.2.2.5.2  | Special requirements applying to forked responses .....  | 670 |
| E.2.2.5.3  | Unsuccessful situations .....  | 670 |
| E.2.2.6    | Emergency service.....   | 671 |
| E.2A       | Usage of SDP .....   | 671 |
| E.2A.0     | General .....  | 671 |
| E.2A.1     | Impact on SDP offer / answer of activation or modification of xDSL bearer for media by the network .....   | 671 |
| E.2A.2     | Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE.....   | 671 |
| E.2A.3     | Emergency service .....  | 671 |
| E.3        | Application usage of SIP.....  | 671 |
| E.3.1      | Procedures at the UE .....   | 671 |
| E.3.1.1    | P-Access-Network-Info header field .....   | 671 |
| E.3.1.2    | Availability for calls .....   | 671 |
| E.3.1.2A   | Availability for SMS.....  | 671 |
| E.3.1.3    | Authorization header field .....   | 671 |
| E.3.1.4    | SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE ..... | 672 |
| E.3.2      | Procedures at the P-CSCF .....   | 672 |
| E.3.2.1    | Determining network to which the originating user is attached.....   | 672 |
| E.3.2.2    | Location information handling .....  | 672 |
| E.3.3      | Procedures at the S-CSCF .....   | 672 |
| E.3.3.1    | Notification of AS about registration status.....  | 672 |
| E.4        | 3GPP specific encoding for SIP header field extensions .....   | 672 |
| E.5        | Use of circuit-switched domain.....  | 673 |

**Annex F (normative): Additional procedures in support for hosted NAT .....674**

|                               |   |            |
|-------------------------------|---|------------|
| F.1                           | Scope .....   | 674        |
| F.2                           | Application usage of SIP .....  | 674        |
| F.2.1                         | UE usage of SIP .....   | 674        |
| F.2.1.1                       | General .....   | 674        |
| F.2.1.2                       | Registration and authentication .....   | 674        |
| F.2.1.2.1                     | General .....   | 674        |
| F.2.1.2.1A                    | Parameters contained in the ISIM .....  | 674        |
| F.2.1.2.1B                    | Parameters provisioned to a UE without ISIM or USIM .....   | 674        |
| F.2.1.2.2                     | Initial registration .....  | 674        |
| F.2.1.2.3                     | Initial subscription to the registration-state event package .....  | 676        |
| F.2.1.2.4                     | User-initiated re-registration .....  | 676        |
| F.2.1.2.5                     | Authentication .....  | 676        |
| F.2.1.2.5.1                   | IMS AKA - general .....   | 676        |
| F.2.1.2.5.2                   | Void .....  | 677        |
| F.2.1.2.5.3                   | IMS AKA abnormal cases .....  | 677        |
| F.2.1.2.5.4                   | SIP digest – general .....  | 677        |
| F.2.1.2.5.5                   | SIP digest – abnormal procedures .....  | 677        |
| F.2.1.2.5.6                   | SIP digest with TLS – general .....   | 677        |
| F.2.1.2.5.7                   | SIP digest with TLS – abnormal procedures .....   | 677        |
| F.2.1.2.5.8                   | Abnormal procedures for all security mechanisms .....   | 677        |
| F.2.1.2.5A                    | Network-initiated re-authentication .....   | 677        |
| F.2.1.2.5B                    | Change of IPv6 address due to privacy .....   | 677        |
| F.2.1.2.6                     | User-initiated deregistration .....   | 677        |
| F.2.1.2.7                     | Network-initiated deregistration .....  | 678        |
| F.2.1.3                       | Subscription and notification .....   | 678        |
| F.2.1.4                       | Generic procedures applicable to all methods excluding the REGISTER method .....                          | 678        |
| F.2.1.4.1                     | UE originating case .....   | 678        |
| F.2.1.4.2                     | UE terminating case .....   | 679        |
| F.2.2                         | P-CSCF usage of SIP .....   | 679        |
| F.2.2.1                       | Introduction .....  | 679        |
| F.2.2.2                       | Registration .....  | 679        |
| F.2.3                         | S-CSCF usage of SIP .....   | 682        |
| F.2.3.1                       | S-CSCF usage of SIP .....   | 682        |
| F.2.3.1.1                     | Protected REGISTER with IMS AKA as a security mechanism .....   | 682        |
| F.3                           | Void .....  | 682        |
| F.4                           | P-CSCF usage of SIP in case UDP encapsulated IPsec is not employed .....                                  | 682        |
| F.4.1                         | Introduction .....  | 682        |
| F.4.2                         | Registration .....  | 682        |
| F.4.3                         | General treatment for all dialogs and standalone transactions excluding the REGISTER method .....         | 683        |
| F.4.3.1                       | Introduction .....  | 683        |
| F.4.3.2                       | Request initiated by the UE .....   | 683        |
| F.4.3.3                       | Request terminated by the UE .....  | 684        |
| F.5                           | NAT traversal for media flows .....   | 684        |
| <b>Annex G (informative):</b> | <b>Void .....</b>   | <b>686</b> |
| <b>Annex H (normative):</b>   | <b>IP-Connectivity Access Network specific concepts when using DOCSIS to access IM CN subsystem .....</b> | <b>687</b> |
| H.1                           | Scope .....   | 687        |
| H.2                           | DOCSIS aspects when connected to the IM CN subsystem .....  | 687        |
| H.2.1                         | Introduction .....  | 687        |
| H.2.2                         | Procedures at the UE .....  | 687        |
| H.2.2.1                       | Activation and P-CSCF discovery .....   | 687        |
| H.2.2.1A                      | Modification of IP-CAN used for SIP signalling .....  | 687        |
| H.2.2.1B                      | Re-establishment of the IP-CAN used for SIP signalling .....  | 687        |
| H.2.2.1C                      | P-CSCF restoration procedure .....  | 687        |
| H.2.2.2                       | Void .....  | 688        |
| H.2.2.3                       | Void .....  | 688        |

|                             |  |            |
|-----------------------------|--|------------|
| H.2.2.4                     | Void .....   | 688        |
| H.2.2.5                     | Handling of the IP-CAN for media.....  | 688        |
| H.2.2.5.1                   | General requirements .....   | 688        |
| H.2.2.5.1A                  | Activation or modification of IP-CAN for media by the UE .....   | 688        |
| H.2.2.5.1B                  | Activation or modification of IP-CAN for media by the network.....   | 688        |
| H.2.2.5.1C                  | Deactivation of IP-CAN for media .....   | 688        |
| H.2.2.5.2                   | Special requirements applying to forked responses .....  | 688        |
| H.2.2.5.3                   | Unsuccessful situations .....  | 688        |
| H.2.2.6                     | Emergency service.....   | 688        |
| H.2A                        | Usage of SDP .....   | 688        |
| H.2A.0                      | General .....  | 688        |
| H.2A.1                      | Impact on SDP offer / answer of activation or modification of IP-CAN for media by the network.....   | 688        |
| H.2A.2                      | Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE .....  | 688        |
| H.2A.3                      | Emergency service .....  | 689        |
| H.3                         | Application usage of SIP .....   | 689        |
| H.3.1                       | Procedures at the UE .....   | 689        |
| H.3.1.1                     | P-Access-Network-Info header field .....   | 689        |
| H.3.1.2                     | Availability for calls .....   | 689        |
| H.3.1.2A                    | Availability for SMS.....  | 689        |
| H.3.1.3                     | Authorization header field .....   | 689        |
| H.3.1.4                     | SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE ..... | 689        |
| H.3.2                       | Procedures at the P-CSCF .....   | 689        |
| H.3.2.1                     | Determining network to which the originating user is attached.....   | 689        |
| H.3.2.2                     | Location information handling .....  | 690        |
| H.3.3                       | Procedures at the S-CSCF .....   | 690        |
| H.3.3.1                     | Notification of AS about registration status.....  | 690        |
| H.4                         | 3GPP specific encoding for SIP header field extensions .....   | 690        |
| H.5                         | Use of circuit-switched domain.....  | 690        |
| <b>Annex I (normative):</b> | <b>Additional routing capabilities in support of transit, roaming and interconnection traffics in IM CN subsystem.....</b>   | <b>691</b> |
| I.1                         | Scope.....   | 691        |
| I.1A                        | General .....  | 691        |
| I.2                         | Transit and interconnection routing procedures .....   | 692        |
| I.3                         | Providing IMS application services in support of transit & interconnection traffics .....  | 692        |
| I.3.1                       | Introduction .....   | 692        |
| I.3.2                       | Procedures .....   | 693        |
| I.3.2.1                     | Treatment for dialog and standalone transactions.....  | 693        |
| I.3.2.1A                    | Handling of header fields related to charging .....  | 694        |
| I.3.2.2                     | Original dialog identifier for transit function.....   | 694        |
| I.4                         | Loopback routing procedures .....  | 695        |
| I.4.1                       | Introduction .....   | 695        |
| I.4.2                       | TRF procedure.....   | 695        |
| I.5                         | Overload control.....  | 696        |
| I.5.1                       | Introduction .....   | 696        |
| I.5.2                       | Outgoing subscriptions to load-control event.....  | 696        |
| <b>Annex J (normative):</b> | <b>Void .....</b>  | <b>698</b> |
| <b>Annex K (normative):</b> | <b>Additional procedures in support of UE managed NAT traversal .....</b>  | <b>699</b> |
| K.1                         | Scope.....   | 699        |
| K.2                         | Application usage of SIP.....  | 699        |

|              |  |     |
|--------------|--|-----|
| K.2.1        | Procedures at the UE .....   | 699 |
| K.2.1.1      | General.....   | 699 |
| K.2.1.2      | Registration and authentication.....   | 699 |
| K.2.1.2.1    | General .....  | 699 |
| K.2.1.2.1A   | Parameters contained in the ISIM .....   | 699 |
| K.2.1.2.1B   | Parameters provisioned to a UE without ISIM or USIM .....                        | 699 |
| K.2.1.2.2    | Initial registration.....  | 699 |
| K.2.1.2.2.1  | General .....  | 699 |
| K.2.1.2.2.2  | Initial registration using IMS AKA .....   | 700 |
| K.2.1.2.2.3  | Initial registration using SIP digest without TLS .....                          | 701 |
| K.2.1.2.2.4  | Initial registration using SIP digest with TLS .....                             | 701 |
| K.2.1.2.2.5  | Initial registration using NASS-IMS bundled authentication.....                  | 701 |
| K.2.1.2.3    | Initial subscription to the registration-state event package .....               | 701 |
| K.2.1.2.4    | User-initiated re-registration .....   | 701 |
| K.2.1.2.4.1  | General .....  | 701 |
| K.2.1.2.4.2  | IMS AKA as a security mechanism.....   | 702 |
| K.2.1.2.4.3  | SIP Digest without TLS as a security mechanism.....                              | 702 |
| K.2.1.2.4.4  | SIP Digest with TLS as a security mechanism .....                                | 702 |
| K.2.1.2.4.5  | NASS-IMS bundled authentication as a security mechanism .....                    | 702 |
| K.2.1.2.5    | Authentication.....  | 702 |
| K.2.1.2.5.1  | IMS AKA – general.....   | 702 |
| K.2.1.2.5.2  | Void.....  | 703 |
| K.2.1.2.5.3  | IMS AKA abnormal cases.....  | 703 |
| K.2.1.2.5.4  | SIP digest without TLS – general.....  | 703 |
| K.2.1.2.5.5  | SIP digest without TLS – abnormal procedures .....                               | 703 |
| K.2.1.2.5.6  | SIP digest with TLS – general .....  | 703 |
| K.2.1.2.5.7  | SIP digest with TLS – abnormal procedures .....                                  | 703 |
| K.2.1.2.5.8  | NASS-IMS bundled authentication – general .....                                  | 703 |
| K.2.1.2.5.9  | NASS-IMS bundled authentication – abnormal procedures.....                       | 703 |
| K.2.1.2.5.10 | Abnormal procedures for all security mechanisms.....                             | 703 |
| K.2.1.2.5A   | Network initiated re-authentication.....   | 703 |
| K.2.1.2.5B   | Change of IPv6 address due to privacy.....                                       | 703 |
| K.2.1.2.6    | User-initiated deregistration.....   | 703 |
| K.2.1.2.6.1  | General .....  | 703 |
| K.2.1.2.6.2  | IMS AKA as a security mechanism.....   | 704 |
| K.2.1.2.6.3  | SIP digest as a security mechanism.....  | 704 |
| K.2.1.2.6.4  | SIP digest with TLS as a security mechanism.....                                 | 704 |
| K.2.1.2.6.5  | Initial registration using NASS-IMS bundled authentication.....                  | 704 |
| K.2.1.2.7    | Network-initiated deregistration .....   | 704 |
| K.2.1.3      | Subscription and notification .....  | 704 |
| K.2.1.4      | Generic procedures applicable to all methods excluding the REGISTER method ..... | 704 |
| K.2.1.4.1    | UE-originating case.....   | 704 |
| K.2.1.4.2    | UE-terminating case.....   | 705 |
| K.2.1.5      | Maintaining flows and detecting flow failures .....                              | 705 |
| K.2.1.6      | Emergency services .....   | 706 |
| K.2.1.6.1    | General .....  | 706 |
| K.2.1.6.2    | Initial emergency registration.....  | 706 |
| K.2.1.6.2A   | New initial emergency registration .....   | 706 |
| K.2.1.5A.3   | Initial subscription to the registration-state event package .....               | 706 |
| K.2.1.6.4    | User-initiated emergency reregistration .....                                    | 706 |
| K.2.1.6.5    | Authentication.....  | 706 |
| K.2.1.6.6    | User-initiated emergency deregistration .....                                    | 706 |
| K.2.1.6.7    | Network-initiated emergency deregistration .....                                 | 706 |
| K.2.1.6.8    | Emergency session setup.....   | 706 |
| K.2.1.6.8.1  | General .....  | 706 |
| K.2.1.6.8.2  | Emergency session set-up in case of no registration .....                        | 706 |
| K.2.1.6.8.3  | Emergency session set-up with an emergency registration .....                    | 706 |
| K.2.1.6.8.4  | Emergency session set-up within a non-emergency registration.....                | 706 |
| K.2.1.6.9    | Emergency session release.....   | 706 |
| K.2.2        | Procedures at the P-CSCF .....   | 707 |
| K.2.2.1      | Introduction.....  | 707 |
| K.2.2.2      | Registration.....  | 707 |

|                             |  |            |
|-----------------------------|--|------------|
| K.2.2.2.1                   | General .....  | 707        |
| K.2.2.2.2                   | IMS AKA as a security mechanism .....  | 707        |
| K.2.2.2.3                   | SIP digest without TLS as a security mechanism .....   | 708        |
| K.2.2.2.4                   | SIP digest with TLS as a security mechanism.....   | 709        |
| K.2.2.2.5                   | NASS-IMS bundled authentication as a security mechanism.....   | 709        |
| K.2.2.3                     | General treatment for all dialogs and standalone transactions excluding the REGISTER method.....                                 | 709        |
| K.2.2.3.1                   | Requests initiated by the UE .....   | 709        |
| K.2.2.3.1.1                 | General for all requests.....  | 709        |
| K.2.2.3.1.2                 | General for all responses .....  | 709        |
| K.2.2.3.1.2A                | Abnormal cases .....   | 709        |
| K.2.2.3.1.3                 | Initial request for a dialog.....  | 709        |
| K.2.2.3.1.4                 | Responses to an initial request for a dialog .....   | 709        |
| K.2.2.3.1.5                 | Target refresh request for a dialog.....   | 709        |
| K.2.2.3.1.6                 | Responses to a target refresh request for a dialog .....   | 709        |
| K.2.2.3.1.7                 | Request for a standalone transaction .....   | 709        |
| K.2.2.3.1.8                 | Responses to a request for a standalone transaction .....  | 709        |
| K.2.2.3.1.9                 | Subsequent request other than a target refresh request .....   | 709        |
| K.2.2.3.1.10                | Responses to a subsequent request other than a target refresh request .....  | 710        |
| K.2.2.3.1.11                | Request for an unknown method that does not relate to an existing dialog.....  | 710        |
| K.2.2.3.1.12                | Responses to a request for an unknown method that does not relate to an existing dialog .....                                    | 710        |
| K.2.2.3.2                   | Requests terminated by the UE .....  | 710        |
| K.2.2.3.2.1                 | General for all requests.....  | 710        |
| K.2.2.3.2.2                 | General for all responses .....  | 710        |
| K.2.2.3.2.3                 | Initial request for a dialog.....  | 710        |
| K.2.2.3.2.4                 | Responses to an initial request for a dialog .....   | 710        |
| K.2.2.3.2.5                 | Target refresh request for a dialog.....   | 710        |
| K.2.2.3.2.6                 | Responses to a target refresh request for a dialog .....   | 710        |
| K.2.2.3.2.7                 | Request for a standalone transaction .....   | 710        |
| K.2.2.3.2.8                 | Responses to a request for a standalone transaction .....  | 710        |
| K.2.2.3.2.9                 | Subsequent request other than a target refresh request .....   | 710        |
| K.2.2.3.2.10                | Responses to a subsequent request other than a target refresh request.....   | 711        |
| K.2.2.3.2.11                | Request for an unknown method that does not relate to an existing dialog.....  | 711        |
| K.2.2.3.2.12                | Responses to a request for an unknown method that does not relate to an existing dialog .....                                    | 711        |
| K.2.2.4                     | Void .....   | 711        |
| K.2.2.5                     | Emergency services .....   | 711        |
| K.2.2.5.1                   | General .....  | 711        |
| K.2.2.5.2                   | General treatment for all dialogs and standalone transactions excluding the REGISTER method –<br>from an unregistered user.....  | 711        |
| K.2.2.5.3                   | General treatment for all dialogs and standalone transactions excluding the REGISTER method<br>after emergency registration..... | 711        |
| K.2.2.5.4                   | General treatment for all dialogs and standalone transactions excluding the REGISTER method –<br>non-emergency registration..... | 711        |
| K.2.2.5.5                   | Abnormal cases .....   | 712        |
| K.2.3                       | Void.....  | 712        |
| K.2.4                       | Void.....  | 712        |
| K.3                         | Application usage of SDP .....   | 712        |
| K.3.1                       | UE usage of SDP.....   | 712        |
| K.3.2                       | P-CSCF usage of SDP.....   | 712        |
| K.4                         | Void.....  | 712        |
| K.5                         | Application usage of ICE .....   | 712        |
| K.5.1                       | Introduction .....   | 712        |
| K.5.2                       | UE usage of ICE.....   | 712        |
| K.5.2.1                     | General.....   | 712        |
| K.5.2.2                     | Call initiation – UE-origination case .....  | 712        |
| K.5.2.3                     | Call termination – UE-termination case.....  | 713        |
| K.5.3                       | P-CSCF support of ICE.....   | 714        |
| K.5.4                       | Void.....  | 714        |
| <b>Annex L (normative):</b> | <b>IP-Connectivity Access Network specific concepts when using EPS to<br/>access IM CN subsystem .....</b>                       | <b>715</b> |

|   |  |            |
|---|--|------------|
| L.1   | Scope .....  | 715        |
| L.2   | EPS aspects when connected to the IM CN subsystem via E-UTRAN .....  | 715        |
| L.2.1   | Introduction .....   | 715        |
| L.2.2   | Procedures at the UE .....   | 715        |
| L.2.2.1   | EPS bearer context activation and P-CSCF discovery .....   | 715        |
| L.2.2.1A  | Modification of a EPS bearer context used for SIP signalling .....   | 717        |
| L.2.2.1B  | Re-establishment of the EPS bearer context for SIP signalling .....  | 717        |
| L.2.2.1C  | P-CSCF restoration procedure .....   | 718        |
| L.2.2.2   | Session management procedures .....  | 718        |
| L.2.2.3   | Mobility management procedures .....   | 718        |
| L.2.2.4   | Cell selection and lack of coverage .....  | 718        |
| L.2.2.5   | EPS bearer contexts for media .....  | 719        |
| L.2.2.5.1   | General requirements .....   | 719        |
| L.2.2.5.1A  | Activation or modification of EPS bearer contexts for media by the UE .....  | 719        |
| L.2.2.5.1B  | Activation or modification of EPS bearer contexts for media by the network .....   | 719        |
| L.2.2.5.1C  | Deactivation of EPS bearer context for media .....   | 719        |
| L.2.2.5.2   | Special requirements applying to forked responses .....  | 719        |
| L.2.2.5.3   | Unsuccessful situations .....  | 720        |
| L.2.2.6   | Emergency service .....  | 720        |
| L.2A  | Usage of SDP .....   | 721        |
| L.2A.0  | General .....  | 721        |
| L.2A.1  | Impact on SDP offer / answer of activation or modification of EPS bearer context for media by the network .....  | 722        |
| L.2A.2  | Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE .....  | 722        |
| L.2A.3  | Emergency service .....  | 722        |
| L.3   | Application usage of SIP .....   | 722        |
| L.3.1   | Procedures at the UE .....   | 722        |
| L.3.1.1   | P-Access-Network-Info header field .....   | 722        |
| L.3.1.2   | Availability for calls .....   | 722        |
| L.3.1.2A  | Availability for SMS .....   | 724        |
| L.3.1.3   | Authorization header field .....   | 724        |
| L.3.1.4   | SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE ..... | 724        |
| L.3.2   | Procedures at the P-CSCF .....   | 724        |
| L.3.2.1   | Determining network to which the originating user is attached .....  | 724        |
| L.3.2.2   | Location information handling .....  | 725        |
| L.3.2.3   | Prohibited usage of PDN connection for emergency bearer services .....   | 725        |
| L.3.3   | Procedures at the S-CSCF .....   | 725        |
| L.3.3.1   | Notification of AS about registration status .....   | 725        |
| L.4   | 3GPP specific encoding for SIP header field extensions .....   | 725        |
| L.4.1   | Void .....   | 725        |
| L.5   | Use of circuit-switched domain .....   | 725        |
| <b>Annex M (normative): IP-Connectivity Access Network specific concepts when using cdma2000<sup>®</sup> packet data subsystem to access IM CN subsystem.....</b> |  | <b>726</b> |
| M.1   | Scope .....  | 726        |
| M.2   | cdma2000 <sup>®</sup> packet data subsystem aspects when connected to the IM CN subsystem .....  | 726        |
| M.2.1   | Introduction .....   | 726        |
| M.2.2   | Procedures at the UE .....   | 726        |
| M.2.2.1   | Establishment of IP-CAN bearer and P-CSCF discovery .....  | 726        |
| M.2.2.1A  | Modification of IP-CAN used for SIP signalling .....   | 727        |
| M.2.2.1B  | Re-establishment of the IP-CAN used for SIP signalling .....   | 727        |
| M.2.2.1C  | P-CSCF restoration procedure .....   | 727        |
| M.2.2.2   | Void .....   | 727        |
| M.2.2.3   | IP-CAN bearer control point support of DHCP based P-CSCF discovery .....   | 727        |



|   |  |            |
|---|--|------------|
| M.2.2.4   | Void .....   | 728        |
| M.2.2.5   | Handling of the IP-CAN for media.....  | 728        |
| M.2.2.5.1   | General requirements .....   | 728        |
| M.2.2.5.1A  | Activation or modification of IP-CAN for media by the UE .....   | 728        |
| M.2.2.5.1B  | Activation or modification of IP-CAN for media by the network.....   | 728        |
| M.2.2.5.1C  | Deactivation of IP-CAN for media .....   | 728        |
| M.2.2.5.2   | Special requirements applying to forked responses .....  | 728        |
| M.2.2.5.3   | Unsuccessful situations .....  | 728        |
| M.2.2.6   | Emergency service.....   | 728        |
| M.2A  | Usage of SDP .....   | 728        |
| M.2A.0  | General .....  | 728        |
| M.2A.1  | Impact on SDP offer / answer of activation or modification of IP-CAN for media by the network .....  | 728        |
| M.2A.2  | Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE.....   | 729        |
| M.2A.3  | Emergency service .....  | 729        |
| M.3   | Application usage of SIP .....   | 729        |
| M.3.1   | Procedures at the UE .....   | 729        |
| M.3.1.1   | P-Access-Network-Info header field .....   | 729        |
| M.3.1.2   | Availability for calls .....   | 729        |
| M.3.1.2A  | Availability for SMS.....  | 729        |
| M.3.1.3   | Authorization header field .....   | 729        |
| M.3.1.4   | SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE ..... | 729        |
| M.3.2   | Procedures at the P-CSCF .....   | 729        |
| M.3.2.1   | Determining network to which the originating user is attached.....   | 729        |
| M.3.2.2   | Location information handling .....  | 730        |
| M.3.3   | Procedures at the S-CSCF .....   | 730        |
| M.3.3.1   | Notification of AS about registration status.....  | 730        |
| M.4   | 3GPP specific encoding for SIP header field extensions .....   | 730        |
| M.4.1   | Void.....  | 730        |
| M.5   | Use of circuit switched domain .....   | 730        |
| <b>Annex N (Normative):      Functions to support overlap signalling.....</b>   |  | <b>731</b> |
| N.1   | Scope .....  | 731        |
| N.2   | Digit collection function.....   | 731        |
| N.2.1   | General .....  | 731        |
| N.2.2   | Collection of digits .....   | 731        |
| N.2.2.1   | Initial INVITE request.....  | 731        |
| N.2.2.2   | Collection of additional digits.....   | 732        |
| N.2.2.3   | Handling of 404 (Not Found) / 484 (Address Incomplete) responses .....   | 732        |
| N.2.3   | Forwarding of SIP messages by the digit collection function .....  | 732        |
| N.3   | En-bloc conversion function .....  | 733        |
| N.3.1   | General .....  | 733        |
| N.3.2   | Multiple-INVITE method.....  | 733        |
| N.3.3   | In-dialog method .....   | 734        |
| <b>Annex O (normative):      IP-Connectivity Access Network specific concepts when using the EPC via cdma2000® HRPD to access IM CN subsystem .....</b> |  | <b>736</b> |
| O.1   | Scope.....   | 736        |
| O.2   | IP-CAN aspects when connected to the IM CN subsystem .....   | 736        |
| O.2.1   | Introduction .....   | 736        |
| O.2.2   | Procedures at the UE .....   | 736        |
| O.2.2.1   | IP-CAN bearer context activation and P-CSCF discovery .....  | 736        |
| O.2.2.1A  | Modification of an IP-CAN bearer context used for SIP signalling .....   | 737        |
| O.2.2.1B  | Re-establishment of the IP-CAN bearer context for SIP signalling.....  | 737        |
| O.2.2.1C  | P-CSCF restoration procedure .....   | 738        |

|                               |  |            |
|-------------------------------|--|------------|
| O.2.2.2                       | Session management procedures .....  | 738        |
| O.2.2.3                       | Mobility management procedures.....  | 738        |
| O.2.2.4                       | Cell selection and lack of coverage.....   | 738        |
| O.2.2.5                       | IP-CAN bearer contexts for media .....   | 738        |
| O.2.2.5.1                     | General requirements .....   | 738        |
| O.2.2.5.1A                    | Activation or modification of IP-CAN bearer contexts for media by the UE .....   | 738        |
| O.2.2.5.1B                    | Activation or modification of IP-CAN bearer contexts for media by the network .....  | 738        |
| O.2.2.5.1C                    | Deactivation of of IP-CAN bearer contexts for media .....  | 739        |
| O.2.2.5.2                     | Special requirements applying to forked responses .....  | 739        |
| O.2.2.5.3                     | Unsuccessful situations .....  | 739        |
| O.2.2.6                       | Emergency service.....   | 739        |
| O.2A                          | Usage of SDP .....   | 739        |
| O.2A.0                        | General .....  | 739        |
| O.2A.1                        | Impact on SDP offer / answer of activation or modification of IP-CAN bearer context for media by the network.....  | 739        |
| O.2A.2                        | Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE.....   | 740        |
| O.2A.3                        | Emergency service .....  | 740        |
| O.3                           | Application usage of SIP.....  | 740        |
| O.3.1                         | Procedures at the UE .....   | 740        |
| O.3.1.1                       | P-Access-Network-Info header field .....   | 740        |
| O.3.1.2                       | Availability for calls .....   | 740        |
| O.3.1.2A                      | Availability for SMS.....  | 740        |
| O.3.1.3                       | Authorization header field .....   | 740        |
| O.3.1.4                       | SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE ..... | 741        |
| O.3.2                         | Procedures at the P-CSCF .....   | 741        |
| O.3.2.1                       | Determining network to which the originating user is attached.....   | 741        |
| O.3.2.2                       | Location information handling .....  | 741        |
| O.3.3                         | Procedures at the S-CSCF.....  | 741        |
| O.4                           | 3GPP specific encoding for SIP header field extensions .....   | 741        |
| O.4.1                         | Void.....  | 741        |
| O.5                           | Use of circuit-switched domain.....  | 741        |
| <b>Annex P (informative):</b> | <b>Void .....</b>  | <b>742</b> |
| <b>Annex Q (normative):</b>   | <b>IP-Connectivity Access Network specific concepts when using the cdma2000<sup>®</sup> 1x Femtocell Network to access IM CN subsystem .....</b>   | <b>743</b> |
| Q.1                           | Scope .....  | 743        |
| Q.2                           | cdma2000 <sup>®</sup> 1x Femtocell Network aspects when connected to the IM CN subsystem .....   | 743        |
| Q.2.1                         | Introduction .....   | 743        |
| Q.2.2                         | Procedures at the UE .....   | 743        |
| Q.2.2.1                       | Activation and P-CSCF discovery.....   | 743        |
| Q.2.2.1A                      | Modification of IP-CAN used for SIP signalling.....  | 743        |
| Q.2.2.1B                      | Re-establishment of IP-CAN used for SIP signalling.....  | 744        |
| Q.2.2.2                       | Void .....   | 744        |
| Q.2.2.3                       | Void .....   | 744        |
| Q.2.2.4                       | Void .....   | 744        |
| Q.2.2.5                       | Handling of the IP-CAN for media.....  | 744        |
| Q.2.2.5.1                     | General requirements .....   | 744        |
| Q.2.2.5.1A                    | Activation or modification of IP-CAN for media by the UE .....   | 744        |
| Q.2.2.5.1B                    | Activation or modification of IP-CAN for media by the network.....   | 744        |
| Q.2.2.5.1C                    | Deactivation of IP-CAN for media .....   | 744        |
| Q.2.2.5.2                     | Special requirements applying to forked responses .....  | 744        |
| Q.2.2.5.3                     | Unsuccessful situations .....  | 744        |
| Q.2.2.6                       | Emergency service.....   | 744        |
| Q.2A                          | Usage of SDP .....   | 744        |

|                             |  |            |
|-----------------------------|--|------------|
| Q.2A.0                      | General .....  | 744        |
| Q.2A.1                      | Impact on SDP offer / answer of activation or modification of IP-CAN for media by the network .....  | 744        |
| Q.2A.2                      | Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE.....   | 744        |
| Q.2A.3                      | Emergency service .....  | 745        |
| Q.3                         | Application usage of SIP .....   | 745        |
| Q.3.1                       | Procedures at the UE .....   | 745        |
| Q.3.1.1                     | P-Access-Network-Info header field .....   | 745        |
| Q.3.1.2                     | Availability for calls .....   | 745        |
| Q.3.1.2A                    | Availability for SMS.....  | 745        |
| Q.3.1.3                     | Authorization header field .....   | 745        |
| Q.3.1.4                     | SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE ..... | 745        |
| Q.3.2                       | Procedures at the P-CSCF .....   | 745        |
| Q.3.2.1                     | Determining network to which the originating user is attached.....   | 745        |
| Q.3.2.2                     | Location information handling .....  | 745        |
| Q.3.3                       | Procedures at the S-CSCF .....   | 745        |
| Q.3.3.1                     | Notification of AS about registration status.....  | 745        |
| Q.4                         | 3GPP specific encoding for SIP header field extensions .....   | 745        |
| Q.5                         | Use of circuit-switched domain.....  | 746        |
| <b>Annex R (normative):</b> | <b>IP-Connectivity Access Network specific concepts when using the EPC via WLAN to access IM CN subsystem.....</b>   | <b>747</b> |
| R.1                         | Scope .....  | 747        |
| R.2                         | IP-CAN aspects when connected to the IM CN subsystem .....   | 747        |
| R.2.1                       | Introduction .....   | 747        |
| R.2.2                       | Procedures at the UE .....   | 747        |
| R.2.2.1                     | Establishment of IP-CAN bearer and P-CSCF discovery .....  | 747        |
| R.2.2.1A                    | Modification of an IP-CAN used for SIP signalling.....   | 748        |
| R.2.2.1B                    | Re-establishment of the IP-CAN used for SIP signalling.....  | 748        |
| R.2.2.1C                    | P-CSCF restoration procedure .....   | 748        |
| R.2.2.2                     | Void .....   | 748        |
| R.2.2.3                     | IP-CAN support of DHCP based P-CSCF discovery .....  | 748        |
| R.2.2.4                     | Void .....   | 749        |
| R.2.2.5                     | Tunnel procedures for media .....  | 749        |
| R.2.2.5.1                   | General requirements .....   | 749        |
| R.2.2.5.1A                  | Modification of tunnel for media by the UE .....   | 749        |
| R.2.2.5.1B                  | Modification of tunnel for media by the network .....  | 749        |
| R.2.2.5.1C                  | Deactivation of tunnel for media.....  | 749        |
| R.2.2.5.2                   | Special requirements applying to forked responses .....  | 749        |
| R.2.2.5.3                   | Unsuccessful situations .....  | 749        |
| R.2.2.6                     | Emergency service .....  | 749        |
| R.2A                        | Usage of SDP .....   | 749        |
| R.2A.0                      | General .....  | 749        |
| R.2A.1                      | Impact on SDP offer / answer of activation or modification of IP-CAN for media by the network .....  | 750        |
| R.2A.2                      | Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE.....   | 750        |
| R.2A.3                      | Emergency service .....  | 750        |
| R.3                         | Application usage of SIP .....   | 750        |
| R.3.1                       | Procedures at the UE .....   | 750        |
| R.3.1.1                     | P-Access-Network-Info header field .....   | 750        |
| R.3.1.2                     | Availability for calls .....   | 750        |
| R.3.1.2A                    | Availability for SMS.....  | 750        |
| R.3.1.3                     | Authorization header field .....   | 750        |

|  |  |     |
|--|--|-----|
| R.3.1.4  | SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE ..... | 750 |
| R.3.2  | Procedures at the P-CSCF .....   | 751 |
| R.3.2.1  | Determining network to which the originating user is attached.....   | 751 |
| R.3.2.2  | Location information handling .....  | 751 |
| R.3.3  | Procedures at the S-CSCF .....   | 751 |
| R.3.3.1  | Notification of AS about registration status.....  | 751 |
| R.4  | 3GPP specific encoding for SIP header field extensions .....   | 751 |
| R.5  | Use of circuit-switched domain.....  | 751 |
| <b>Annex S (normative): IP-Connectivity Access Network specific concepts when using DVB-RCS2 to access IM CN subsystem .....</b> |  |     |
| <b>752</b>   |  |     |
| S.1  | Scope .....  | 752 |
| S.2  | DVB-RCS2 aspects when connected to the IM CN subsystem .....   | 752 |
| S.2.1  | Introduction .....   | 752 |
| S.2.2  | Procedures at the UE .....   | 752 |
| S.2.2.1  | Activation and P-CSCF discovery .....  | 752 |
| S.2.2.1A   | Modification of IP-CAN bearer used for SIP signalling.....   | 752 |
| S.2.2.1B   | Re-establishment of IP-CAN bearer used for SIP signalling.....   | 752 |
| S.2.2.1C   | P-CSCF restoration procedure .....   | 752 |
| S.2.2.2  | Void .....   | 753 |
| S.2.2.3  | Void .....   | 753 |
| S.2.2.4  | Void .....   | 753 |
| S.2.2.5  | Handling of the IP-CAN for media.....  | 753 |
| S.2.2.5.1  | General requirements .....   | 753 |
| S.2.2.5.1A   | Activation or modification of IP-CAN for media by the UE .....   | 753 |
| S.2.2.5.1B   | Activation or modification of IP-CAN for media by the network.....   | 753 |
| S.2.2.5.1C   | Deactivation of IP-CAN for media .....   | 753 |
| S.2.2.5.2  | Special requirements applying to forked responses .....  | 753 |
| S.2.2.5.3  | Unsuccessful situations .....  | 753 |
| S.2.2.6  | Emergency service .....  | 753 |
| S.2A   | Usage of SDP .....   | 753 |
| S.2A.0   | General .....  | 753 |
| S.2A.1   | Impact on SDP offer / answer of activation or modification of satellite bearer for media by the network ....   | 753 |
| S.2A.2   | Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE.....   | 753 |
| S.2A.3   | Emergency service .....  | 754 |
| S.3  | Application usage of SIP.....  | 754 |
| S.3.1  | Procedures at the UE .....   | 754 |
| S.3.1.1  | P-Access-Network-Info header field .....   | 754 |
| S.3.1.2  | Availability for calls .....   | 754 |
| S.3.1.2A   | Availability for SMS.....  | 754 |
| S.3.1.3  | Authorization header field .....   | 754 |
| S.3.1.4  | SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE ..... | 754 |
| S.3.2  | Procedures at the P-CSCF .....   | 754 |
| S.3.2.1  | Determining network to which the originating user is attached.....   | 754 |
| S.3.2.2  | Location information handling .....  | 754 |
| S.3.3  | Procedures at the S-CSCF .....   | 755 |
| S.3.3.1  | Notification of AS about registration status.....  | 755 |
| S.4  | 3GPP specific encoding for SIP header field extensions .....   | 755 |
| S.5  | Use of circuit-switched domain.....  | 755 |
| <b>Annex T (informative): Change history .....</b>   |  |     |
| <b>756</b>   |  |     |

History .....822

---

# Foreword

This Technical Specification has been produced by the 3<sup>rd</sup> Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

---

# 1 Scope

The present document defines a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP).

The present document is applicable to:

- the interface between the User Equipment (UE) and the Call Session Control Function (CSCF);
- the interface between the CSCF and any other CSCF;
- the interface between the CSCF and an Application Server (AS);
- the interface between the CSCF and an ISC gateway function;
- the interface between the ISC gateway function and an Application Server (AS);
- the interface between the CSCF and the Media Gateway Control Function (MGCF);
- the interface between the S-CSCF and the Multimedia Resource Function Controller (MRFC);
- the interface between the Application Server (AS) and the Multimedia Resource Function Controller (MRFC);
- the interface between the S-CSCF and the Media Resource Broker (MRB);
- the interface between the AS and the MRB;
- the interface between the MRB and the MRFC;
- the interface between the CSCF and the Breakout Gateway Control Function (BGCF);
- the interface between the BGCF and the MGCF;
- the interface between the CSCF and an IBCF;
- the interface between the IBCF and AS, MRFC or MRB;
- the interface between the E-CSCF and the Location Retrieval Function (LRF);
- the interface between the BGCF and any other BGCF;
- the interface between the CSCF and an external Multimedia IP network;
- the interface between the E-CSCF and the EATF;
- the interface between the P-CSCF and the ATCF;
- the interface between the ATCF and the I-CSCF;
- the interface between the ATCF and the IBCF; and
- the interface between the transit function and the AS.

Where possible the present document specifies the requirements for this protocol by reference to specifications produced by the IETF within the scope of SIP and SDP. Where this is not possible, extensions to SIP and SDP are defined within the present document. The document has therefore been structured in order to allow both forms of specification.

As the IM CN subsystem is designed to interwork with different IP-Connectivity Access Networks (IP-CANs), the IP-CAN independent aspects of the IM CN subsystem are described in the main body and annex A of this specification. Aspects for connecting a UE to the IM CN subsystem through specific types of IP-CANs are documented separately in the annexes or in separate documents.

The document also specifies HTTP for use by an AS and by an MRB in support of the provision of media resources.

The document also specifies media-related requirements for the NAT traversal mechanisms defined in this specification.

NOTE: The present document covers only the usage of SIP and SDP to communicate with the entities of the IM CN subsystem. It is possible, and not precluded, to use the capabilities of IP-CAN to allow a terminal containing a SIP UA to communicate with SIP servers or SIP UAs outside the IM CN subsystem, and therefore utilise the services provided by those SIP servers. The usage of SIP and SDP for communicating with SIP servers or SIP UAs outside the IM CN subsystem is outside the scope of the present document.

---

## 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [1A] 3GPP TS 22.101: "Service aspects; Service principles".
- [1B] 3GPP TS 22.003: "Circuit Teleservices supported by a Public Land Mobile Network (PLMN)".
- [2] 3GPP TS 23.002: "Network architecture".
- [3] 3GPP TS 23.003: "Numbering, addressing and identification".
- [4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".
- [4A] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".
- [4B] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency sessions".
- [4C] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".
- [4D] 3GPP TS 23.140 Release 6: "Multimedia Messaging Service (MMS); Functional description; Stage 2".
- [5] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".
- [6] 3GPP TS 23.221: "Architectural requirements".
- [7] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".
- [7A] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".
- [7B] 3GPP TS 23.401: "GPRS enhancements for E-UTRAN access".
- [7C] 3GPP TS 23.292: "IP Multimedia Subsystem (IMS) Centralized Services; Stage 2".
- [7D] 3GPP TS 23.380: "IMS Restoration Procedures".
- [7E] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".
- [7F] 3GPP TS 23.334: "IMS Application Level Gateway (IMS-ALG) – IMS Access Gateway (IMS-AGW) interface".
- [8] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".
- [8A] 3GPP TS 24.141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".



- [8B] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".
- [8C] 3GPP TS 24.234: "3GPP System to Wireless Local Area Network (WLAN) interworking; WLAN User Equipment (WLAN UE) to network protocols; Stage 3".
- [8D] Void.
- [8E] 3GPP TS 24.279: "Combining Circuit Switched (CS) and IP Multimedia Subsystem (IMS) services, stage 3, Release 7".
- [8F] 3GPP TS 24.247: "Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".
- [8G] 3GPP TS 24.167: "3GPP IMS Management Object (MO); Stage 3".
- [8H] 3GPP TS 24.173: "IMS Multimedia telephony communication service and supplementary services; Stage 3".
- [8I] 3GPP TS 24.606: "Message Waiting Indication (MWI) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".
- [8J] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".
- [8K] Void.
- [8L] 3GPP TS 24.341: "Support of SMS over IP networks; Stage 3".
- [8M] 3GPP TS 24.237: "IP Multimedia Subsystem (IMS) Service Continuity; Stage 3".
- [8N] 3GPP TS 24.647: "Advice Of Charge (AOC) using IP Multimedia (IM) Core Network (CN) subsystem".
- [8O] 3GPP TS 24.292: "IP Multimedia (IM) Core Network (CN) subsystem Centralized Services (ICS); Stage 3".
- [8P] 3GPP TS 24.623: "Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services".
- [8Q] 3GPP TS 24.182: "IP Multimedia Subsystem (IMS) Customized Alerting Tones (CAT); Protocol specification".
- [8R] 3GPP TS 24.183: "IP Multimedia Subsystem (IMS) Customized Ringing Signal (CRS); Protocol specification".
- [8S] 3GPP TS 24.616: "Malicious Communication Identification (MCID) using IP Multimedia (IM) Core Network (CN) subsystem".
- [8T] 3GPP TS 24.305: "Selective Disabling of 3GPP User Equipment Capabilities (SDoUE) Management Object (MO)".
- [8U] 3GPP TS 24.302: "Access to the Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3".
- [8V] 3GPP TS 24.303: "Mobility management based on Dual-Stack Mobile IPv6".
- [8W] 3GPP TS 24.390: "Unstructured Supplementary Service Data (USSD) using IP Multimedia (IM) Core Network (CN) subsystem IMS".
- [8X] 3GPP TS 24.139: "3GPP System-Fixed Broadband Access Network Interworking; Stage 3".
- [8ZC] 3GPP TS 24.337: "IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) inter-UE transfer; Stage 3".
- [9] 3GPP TS 25.304: "User Equipment (UE) procedures in idle mode and procedures for cell reselection in connected mode".

- [9A] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".
- [9B] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction".
- [10] Void.
- [10A] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services".
- [11] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".
- [11A] 3GPP TS 29.162: "Interworking between the IM CN subsystem and IP networks".
- [11B] 3GPP TS 29.163: "Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks".
- [11C] 3GPP TS 29.161: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services with Wireless Local Access and Packet Data Networks (PDN)".
- [11D] 3GPP TS 29.079: "Optimal Media Routeing within the IP Multimedia Subsystem".
- [12] 3GPP TS 29.207 Release 6: "Policy control over Go interface".
- [13] Void.
- [13A] 3GPP TS 29.209 Release 6: "Policy control over Gq interface".
- [13B] 3GPP TS 29.212: "Policy and Charging Control (PCC); Reference points".
- [13C] 3GPP TS 29.213: "Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping".
- [13D] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".
- [14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".
- [15] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".
- [15A] 3GPP TS 29.311: "Service Level Interworking for Messaging Services".
- [15B] 3GPP TS 31.103: "Characteristics of the IP multimedia services identity module (ISIM) application".
- [15C] 3GPP TS 31.102: "Characteristics of the Universal Subscriber Identity Module (USIM) application".
- [15D] 3GPP TS 31.111: "Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)".
- [16] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".
- [17] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".
- [17A] Void.
- [18] 3GPP TS 33.102: "3G Security; Security architecture".
- [19] 3GPP TS 33.203: "Access security for IP based services".
- [19A] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".
- [19B] 3GPP TS 36.304: "Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode".
- [19C] 3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security".

- [20] 3GPP TS 44.018: "Mobile radio interface layer 3 specification; Radio Resource Control (RRC) protocol".
- [20A] RFC 2401 (November 1998): "Security Architecture for the Internet Protocol".
- [20B] RFC 1594 (March 1994): "FYI on Questions and Answers to Commonly asked "New Internet User" Questions".
- [20C] Void.
- [20D] Void.
- [20E] RFC 2462 (November 1998): "IPv6 Stateless Address Autoconfiguration".
- [20F] RFC 2132 (March 1997): "DHCP Options and BOOTP Vendor Extensions".
- [20G] RFC 2234 (November 1997): "Augmented BNF for Syntax Specification: ABNF".
- [21] RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication".
- [22] RFC 3966 (December 2004): "The tel URI for Telephone Numbers".
- [23] RFC 4733 (December 2006): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".
- [24] RFC 6116 (March 2011): "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".
- [25] RFC 6086 (October 2009): "Session Initiation Protocol (SIP) INFO Method and Package Framework".
- [25A] RFC 3041 (January 2001): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".
- [26] RFC 3261 (June 2002): "SIP: Session Initiation Protocol".
- [27] RFC 3262 (June 2002): "Reliability of provisional responses in Session Initiation Protocol (SIP)".
- [27A] RFC 3263 (June 2002): "Session Initiation Protocol (SIP): Locating SIP Servers".
- [27B] RFC 3264 (June 2002): "An Offer/Answer Model with Session Description Protocol (SDP)".
- [28] RFC 3265 (June 2002): "Session Initiation Protocol (SIP) Specific Event Notification".
- [28A] Void.
- [29] RFC 3311 (September 2002): "The Session Initiation Protocol (SIP) UPDATE method".
- [30] RFC 3312 (October 2002): "Integration of resource management and Session Initiation Protocol (SIP)".
- [31] RFC 3313 (January 2003): "Private Session Initiation Protocol (SIP) Extensions for Media Authorization".
- [32] RFC 3320 (March 2002): "Signaling Compression (SigComp)".
- [33] RFC 3323 (November 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".
- [34] RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".
- [34A] RFC 3326 (December 2002): "The Reason Header Field for the Session Initiation Protocol (SIP)".
- [35] RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".
- [35A] RFC 3361 (August 2002): "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

- [36] RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method".
- [37] RFC 3420 (November 2002): "Internet Media Type message/sipfrag".
- [37A] RFC 3605 (October 2003): "Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)".
- [38] RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration".
- [39] RFC 4566 (June 2006): "SDP: Session Description Protocol".
- [40] RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".
- [40A] RFC 2131 (March 1997): "Dynamic host configuration protocol".
- [41] RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".
- [42] RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) static dictionary for Signaling Compression (SigComp)".
- [43] RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".
- [44] Void.
- [45] Void.
- [46] Void.
- [47] Void.
- [48] RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".
- [49] RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".
- [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".
- [51] Void.
- [52] RFC 7315 (July 2014): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP".
- [52A] RFC 7976 (September 2016): "Updates to Private Header (P-Header) Extension Usage in Session Initiation Protocol (SIP) Requests and /Responses".
- [53] RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol".
- [54] RFC 3524 (April 2003): "Mapping of Media Streams to Resource Reservation Flows".
- [55] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)".
- [55A] RFC 3551 (July 2003): "RTP Profile for Audio and Video Conferences with Minimal Control".
- [56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".
- [56A] RFC 3581 (August 2003): "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".
- [56B] RFC 3841 (August 2004): "Caller Preferences for the Session Initiation Protocol (SIP)".
- [56C] RFC 3646 (December 2003): "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".
- [57] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

- [58] RFC 4028 (April 2005): "Session Timers in the Session Initiation Protocol (SIP)".
- [59] RFC 3892 (September 2004): "The Session Initiation Protocol (SIP) Referred-By Mechanism".
- [60] RFC 3891 (September 2004): "The Session Initiation Protocol (SIP) "Replaces" Header".
- [61] RFC 3911 (October 2004): "The Session Initiation Protocol (SIP) "Join" Header".
- [62] RFC 3840 (August 2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)".
- [63] RFC 3861 (August 2004): "Address Resolution for Instant Messaging and Presence".
- [63A] RFC 3948 (January 2005): "UDP Encapsulation of IPsec ESP Packets".
- [64] RFC 4032 (March 2005): "Update to the Session Initiation Protocol (SIP) Preconditions Framework".
- [65] RFC 3842 (August 2004) "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)"
- [65A] RFC 4077 (May 2005): "A Negative Acknowledgement Mechanism for Signaling Compression".
- [66] RFC 4244 (November 2005): "An Extension to the Session Initiation Protocol (SIP) for Request History Information".
- [67] RFC 5079 (December 2007): "Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)".
- [68] RFC 4458 (January 2006): "Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)".
- [69] RFC 5031 (January 2008): "A Uniform Resource Name (URN) for Services".
- [70] RFC 3903 (October 2004): "An Event State Publication Extension to the Session Initiation Protocol (SIP)".
- [71] Void.
- [72] RFC 3857 (August 2004): "A Watcher Information Event Template Package for the Session Initiation Protocol (SIP)".
- [74] RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".
- [74A] RFC 3603 (October 2003): "Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture".
- [74B] RFC 3959 (December 2004): "The Early Session Disposition Type for the Session Initiation Protocol (SIP)".
- [75] RFC 4662 (August 2006): "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists".
- [77] RFC 5875 (May 2010): "An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Diff Event Package".
- [78] RFC 4575 (August 2006): "A Session Initiation Protocol (SIP) Event Package for Conference State".
- [79] RFC 5049 (December 2007): "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)".
- [80] Void.
- [81] Void.

- [82] RFC 4457 (April 2006): "The Session Initiation Protocol (SIP) P-User-Database Private-Header (P-header)".
- [83] RFC 4145 (September 2005): "TCP-Based Media Transport in the Session Description Protocol (SDP)".
- [84] RFC 4320 (January 2006): "Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction".
- [85] 3GPP2 C.S0005-D (March 2004): "Upper Layer (Layer 3) Signaling Standard for cdma2000 Standards for Spread Spectrum Systems".
- [86] 3GPP2 C.S0024-B v3.0 (September 2009): "cdma2000 High Rate Packet Data Air Interface Standard".
- [86A] 3GPP2 C.S0084-000 (April 2007): "Overview for Ultra Mobile Broadband (UMB) Air Interface Specification".
- [86B] 3GPP2 X.S0060-0 v1.0: "HRPD Support for Emergency Services".
- [86C] 3GPP2 X.S0057-B v2.0: "E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects".
- [86D] 3GPP2 C.S0014-C v1.0: "Enhanced Variable Rate Codec, Speech Service Options 3, 68, and 70 for Wideband Spread Spectrum Digital Systems".
- [86E] 3GPP2 X.S0059-200-A v1.0: "cdma2000 Femtocell Network: 1x and IMS Network Aspects".
- [86F] 3GPP2 S.R0048-A v4.0: "3G Mobile Equipment Identifier (MEID) - Stage 1".
- [87] ITU-T Recommendation J.112, "Transmission Systems for Interactive Cable Television Services"
- [88] PacketCable Release 2 Technical Report, PacketCable™ Architecture Framework Technical Report, PKT-TR-ARCH-FRM.
- [89] RFC 6442 (December 2011): "Location Conveyance for the Session Initiation Protocol".
- [90] RFC 4119 (December 2005) "A Presence-based GEOPRIV Location Object Format".
- [91] RFC 5012 (January 2008): "Requirements for Emergency Context Resolution with Internet Technologies".
- [91A] Void.
- [92] RFC 5626 (October 2009): "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)".
- [93] RFC 5627 (October 2009): "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)".
- [94] RFC 5628 (October 2009): "Registration Event Package Extension for Session Initiation Protocol (SIP) Globally Routable User Agent URIs (GRUUs)".
- [95] Void.
- [96] RFC 4168 (October 2005): "The Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)".
- [97] RFC 5002 (August 2007): "The Session Initiation Protocol (SIP) P-Profile-Key Private Header (P-Header)".
- [98] ETSI ES 283 035: "Telecommunications and Internet Converged Services and Protocols for Advanced Networks (TISPAN); Network Attachment Sub-System (NASS); e2 interface based on the DIAMETER protocol".
- [99] RFC 5245 (April 2010): "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols".

- [100] RFC 5389 (October 2008): "Session Traversal Utilities for NAT (STUN)".
- [101] RFC 5766 (April 2010): "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)".
- [102] RFC 5768 (April 2010): "Indicating Support for Interactive Connectivity Establishment (ICE) in the Session Initiation Protocol (SIP)".
- [103] RFC 4967 (July 2007): "Dial String Parameter for the Session Initiation Protocol Uniform Resource Identifier".
- [104] RFC 5365 (October 2008): "Multiple-Recipient MESSAGE Requests in the Session Initiation Protocol (SIP)".
- [105] RFC 5368 (October 2008): "Referring to Multiple Resources in the Session Initiation Protocol (SIP)".
- [106] RFC 5366 (October 2008): "Conference Establishment Using Request-Contained Lists in the Session Initiation Protocol (SIP)".
- [107] RFC 5367 (October 2008): "Subscriptions to Request-Contained Resource Lists in the Session Initiation Protocol (SIP)".
- [108] RFC 4583 (November 2006): "Session Description Protocol (SDP) Format for Binary Floor Control Protocol (BFCP) Streams".
- [109] RFC 5009 (September 2007): "Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media".
- [110] RFC 4354 (January 2006): "A Session Initiation Protocol (SIP) Event Package and Data Format for Various Settings in Support for the Push-to-Talk over Cellular (PoC) Service".
- [111] RFC 4964 (September 2007): "The P-Answer-State Header Extension to the Session Initiation Protocol for the Open Mobile Alliance Push to Talk over Cellular".
- [112] RFC 4694 (October 2006): "Number Portability Parameters for the 'tel' URI".
- [113] Void.
- [114] RFC 4769 (November 2006): "IANA Registration for an Enumservice Containing Public Switched Telephone Network (PSTN) Signaling Information".
- [115] RFC 4411 (February 2006): "Extending the Session Initiation Protocol (SIP) Reason Header for Preemption Events".
- [116] RFC 4412 (February 2006): "Communications Resource Priority for the Session Initiation Protocol (SIP)".
- [117] RFC 5393 (December 2008): "Addressing an Amplification Vulnerability in Session Initiation Protocol (SIP) Forking Proxies".
- [118] RFC 4896 (June 2007): "Signaling Compression (SigComp) Corrections and ClarificationsImplementer's Guide for SigComp".
- [119] RFC 5112 (January 2008): "The Presence-Specific Static Dictionary for Signaling Compression (Sigcomp)".
- [120] RFC 5688 (January 2010): "A Session Initiation Protocol (SIP) Media Feature Tag for MIME Application Subtype".
- [121] RFC 6050 (November 2010): "A Session Initiation Protocol (SIP) Extension for the Identification of Services".
- [122] RFC 4346 (April 2006): "The TLS Protocol Version 1.1".
- [123] Void.

- [124] RFC 3986 (January 2005): "Uniform Resource Identifiers (URI): Generic Syntax".
- [125] RFC 5360 (October 2008): "A Framework for Consent-Based Communications in the Session Initiation Protocol (SIP)".
- [126] RFC 7433 (January 2015): "A Mechanism for Transporting User-to-User Call Control Information in SIP".
- [126A] RFC 7434 (January 2015): "Interworking ISDN Call Control User Information with SIP".
- [127] 3GPP2 X.S0011-E: "cdma2000 Wireless IP Network Standard".
- [130] RFC 6432 (November 2011): "Carrying Q.850 Codes in Reason Header Fields in SIP (Session Initiation Protocol) Responses".
- [131] RFC 6544 (March 2012): "TCP Candidates with Interactive Connectivity Establishment (ICE)".
- [132] RFC 3023 (January 2001): "XML Media Types".
- [133] RFC 5502 (April 2009): "The SIP P-Served-User Private-Header (P-Header) for the 3GPP IP Multimedia (IM) Core Network (CN) Subsystem".
- [134] RFC 7316 (July 2014): "The Session Initiation Protocol (SIP) P-Private-Network-Indication Private Header (P-Header)".
- [135] RFC 4585 (July 2006): "Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)".
- [136] RFC 5104 (February 2008): "Codec Control Messages in the RTP Audio-Visual Profile with Feedback (AVPF)".
- [137] RFC 5939 (September 2010): "Session Description Protocol (SDP) Capability Negotiation".
- [138] ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1".
- [139] Void.
- [140] Void.
- [141] Void.
- [142] RFC 6228 (May 2011): "Response Code for Indication of Terminated Dialog".
- [143] RFC 6223 (April 2011): "Indication of support for keep-alive".
- [144] RFC 4240 (December 2005): "Basic Network Media Services with SIP".
- [145] RFC 5552 (May 2009): "SIP Interface to VoiceXML Media Services".
- [146] RFC 6230 (May 2011): "Media Control Channel Framework".
- [147] RFC 6231 (May 2011): "An Interactive Voice Response (IVR) Control Package for the Media Control Channel Framework".
- [148] RFC 6505 (March 2012): "A Mixer Control Package for the Media Control Channel Framework".
- [149] RFC 2046 (November 1996): "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".
- [150] RFC 5621 (September 2009): "Message Body Handling in the Session Initiation Protocol (SIP)".
- [151] RFC 3862 (August 2004): "Common Presence and Instant Messaging (CPIM): Message Format".
- [152] RFC 3890 (September 2004): "A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)".



- [153] RFC 7254 (May 2014): "A Uniform Resource Name Namespace for the Global System for Mobile Communications Association (GSMA) and the International Mobile station Equipment Identity (IMEI)".
- [154] RFC 4122 (July 2005): "A Universally Unique Identifier (UUID) URN Namespace".
- [155] RFC 7195 (May 2014): "Session Description Protocol (SDP) Extension for Setting Audio Media Streams over Circuit-Switched Bearers in the Public Switched Telephone Network (PSTN)".
- [156] RFC 7006 (September 2013): "Miscellaneous Capabilities Negotiation in the Session Description Protocol (SDP)".
- [157] RFC 5438 (January 2009): "Instant Message Disposition Notification (IMDN)".
- [158] RFC 5373 (November 2008): "Requesting Answering Modes for the Session Initiation Protocol (SIP)".
- [160] Void.
- [161] RFC 4288 (December 2005): "Media Type Specifications and Registration Procedures".
- [162] RFC 7329 (August 2014): "A Session Identifier for the Session Initiation Protocol (SIP)".
- [163] RFC 6026 (September 2010): "Correct Transaction Handling for 2xx Responses to Session Initiation Protocol (SIP) INVITE Requests".
- [164] RFC 5658 (October 2009): "Addressing Record-Route issues in the Session Initiation Protocol (SIP)".
- [165] RFC 5954 (August 2010): "Essential Correction for IPv6 ABNF and URI Comparison in RFC3261".
- [166] RFC 4117 (June 2005): "Transcoding Services Invocation in the Session Initiation Protocol (SIP) using Third Party Call Control (3pcc)".
- [167] RFC 4567 (July 2006): "Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)".
- [168] RFC 4568 (July 2006): "Session Description Protocol (SDP) Security Descriptions for Media Streams".
- [169] RFC 3711 (March 2004): "The Secure Real-time Transport Protocol (SRTP)".
- [170] RFC 6043 (March 2011): "MIKEY-TICKET: Ticket-Based Modes of Key Distribution in Multimedia Internet KEYing (MIKEY)".
- [171] RFC 4235 (November 2005): "An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP)".
- [172] RFC 6871 (February 2013): "SDP media capabilities Negotiation".
- [173] RFC 4488 (May 2006): "Suppression of Session Initiation Protocol (SIP) REFER Method Implicit Subscription".
- [174] Void.
- [175] RFC 7462 (March 2015): "URNs for the Alert-Info Header Field of the Session Initiation Protocol (SIP)".
- [176] ANSI/J-STD-036-B: "Enhanced Wireless 9-1-1, Phase 2".
- [177] Void.
- [178] RFC 4975 (September 2007): "The Message Session Relay Protocol (MSRP)".
- [179] RFC 3859 (August 2004): "Common Profile for Presence (CPP)".

- [180] RFC 3860 (August 2004): "Common Profile for Instant Messaging (CPIM)".
- [181] RFC 2368 (July 1998): "The mailto URL scheme".
- [182] RFC 4745 (February 2007): "Common Policy: A Document Format for Expressing Privacy Preferences".
- [183] RFC 5318 (December 2008): "The Session Initiation Protocol (SIP) P-Refused-URI-List Private-Header (P-Header)".
- [184] RFC 4538 (June 2006): "Request Authorization through Dialog Identification in the Session Initiation Protocol (SIP)".
- [185] RFC 5547 (May 2009): "A Session Description Protocol (SDP) Offer/Answer Mechanism to Enable File Transfer".
- [186] RFC 4483 (May 2006): "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages".
- [187] RFC 8464 (September 2018): "A URN Namespace for Device Identity and Mobile Equipment Identity (MEID)".
- [188] RFC 6679 (August 2012): "Explicit Congestion Notification (ECN) for RTP over UDP".
- [189] RFC 3168 (September 2001): "The Addition of Explicit Congestion Notification (ECN) to IP".
- [190] RFC 6809 (November 2012): "Mechanism to Indicate Support of Features and Capabilities in the Session Initiation Protocol (SIP)".
- [191] RFC 6140 (March 2011): "Registration for Multiple Phone Numbers in the Session Initiation Protocol (SIP)".
- [192] RFC 6917 (April 2013): "Media Resource Brokering".
- [193] ETSI TS 101 454-1 v1.1.1: "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 1: Overview and System Level specification".
- [194] ETSI EN 301 545-2 v1.1.1: "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 2: Lower Layers for Satellite standard".
- [195] ETSI TS 101 545-3 v1.1.1: "Digital Video Broadcasting (DVB); Second Generation DVB Interactive Satellite System (DVB-RCS2); Part 3: Higher Layers Satellite Specification".
- [196] RFC 2616 (June 1999): "Hypertext Transfer Protocol -- HTTP/1.1".
- [197] RFC 7135 (May 2014): "IANA Registering a SIP Resource Priority Header Field Namespace for Local Emergency Communications".
- [198] RFC 6357 (August 2011): "Design Considerations for Session Initiation Protocol (SIP) Overload Control".
- [199] RFC 7339 (September 2014): "Session Initiation Protocol (SIP) Overload Control".
- [200] RFC 7415 (February 2015): "Session Initiation Protocol (SIP) Rate Control".
- [201] RFC 7200 (April 2014): "A Session Initiation Protocol (SIP) Load-Control Event Package".
- [202] ITU-T Recommendation T.38 (September 2010): "Procedures for real-time Group 3 facsimile communication over IP networks".
- [203] ISO 8601 (December 2004): "Date elements and interchange formats – Information interchange – Representation of dates and times".
- [204] RFC 5506 (April 2009): "Support for Reduced-Size Real-Time Transport Control Protocol (RTCP)".
- [205] RFC 3611 (November 2003): "RTP Control Protocol Extended Reports (RTCP XR)".

- [206] RFC 4796 (February 2007): "The Session Description Protocol (SDP) Content Attribute".
- [207] Void.
- [208] Void.
- [209] Void.
- [210] Void.
- [211] Void.
- [212] RFC 20 (May 2011): "ASCII format for Network Interchange".
- [234] RFC 7913 (June 2016): "P-Access-Network-Info ABNF Update".
- [239] draft-ietf-sipcore-originating-cdiv-parameter-07 (November 2018): "P-Served-User Header Field Parameter for Originating CDIV session case in Session Initiation Protocol (SIP)".

Editor's note [WI: IMSProtoc5, CR#5582]: The above document cannot be formally referenced until it is published as an RFC.

---

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

**Entry point:** In the case that "border control concepts", as specified in 3GPP TS 23.228 [7], are to be applied in an IM CN subsystem, then these are to be provided by capabilities within the IBCF, and the IBCF acts as an entry point for this network (instead of the I-CSCF). In this case the IBCF and the I-CSCF can be co-located as a single physical node. If "border control concepts" are not applied, then the I-CSCF is considered as an entry point of a network. If the P-CSCF is in the home network, then the I-CSCF is considered as an entry point for this document. Similarly, in case that "border control concepts", as specified in 3GPP TS 23.218 [5], are to be applied in an ISC interface, then these are to be provided by capabilities within the ISC gateway function, and the ISC gateway function acts as an entry point for this network.

**Exit point:** If operator preference requires the application of "border control concepts" as specified in 3GPP TS 23.228 [7], then these are to be provided by capabilities within the IBCF, and requests sent towards another network are routed via a local network exit point (IBCF), which will then forward the request to the other network (discovering the entry point if necessary). Similarly, in case that "border control concepts", as specified in 3GPP TS 23.218 [5], are to be applied in an ISC interface, then these are to be provided by capabilities within the ISC gateway function, and requests sent towards another network are routed via a local network exit point (ISC gateway function).

**Geo-local number:** Either a geo-local service number as specified in 3GPP TS 23.228 [7] or a number in non-international format according to an addressing plan used at the current physical location of the user.

**Home-local number:** Either a home local service number as specified in 3GPP TS 23.228 [7] or a number in non-international format according to an addressing plan used in the home network of the user.

**Main URI:** In the case that the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI is the URI which is used for the registration procedures in the To header of the REGISTER request as specified in RFC 6140 [191]; it represents the public user identities associated to that UE.

**Newly established set of security associations:** Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF after the 200 (OK) response to a REGISTER request was received.

**Old set of security associations:** Two pairs of IPsec security associations still in existence after another set of security associations has been established due to a successful authentication procedure.

**Temporary set of security associations:** Two pairs of IPsec security associations that have been created at the UE and/or the P-CSCF, after an authentication challenge within a 401 (Unauthorized) response to a REGISTER request was received. The SIP level lifetime of such created security associations will be equal to the value of reg-await-auth timer.

**Integrity protected:** See 3GPP TS 33.203 [19]. Where a requirement exists to send information "integrity-protected" the mechanisms specified in 3GPP TS 33.203 [19] are used for sending the information. Where a requirement exists to check that information was received "integrity-protected", then the information received is checked for compliance with the procedures as specified in 3GPP TS 33.203 [19].

**Instance ID:** An URN generated by the device that uniquely identifies a specific device amongst all other devices, and does not contain any information pertaining to the user (e.g., in GPRS instance ID applies to the Mobile Equipment rather than the UICC). The public user identity together with the instance ID uniquely identifies a specific UA instance. If the device has an IMEI available, it generates an instance ID based on its IMEI as defined in 3GPP TS 23.003 [3] clause 13. If the device has an MEID as defined in 3GPP2 S.R0048-A [86F] available, it generates an instance ID based on its MEID as defined in RFC 8464 [187]. If the device does not have an IMEI available and does not have an MEID available, the instance ID is generated as a string representation of a UUID as a URN as defined in RFC 4122 [154].

**Resource reservation:** Mechanism for reserving bearer resources that is required for certain access technologies.

**Local preconditions:** The indication of segmented status preconditions for the local reservation of resources as specified in RFC 3312 [30].

**Alias URI, Alias SIP URI:** A URI is an alias of another URI if the treatment of both URIs is identical, i.e. both URIs belong to the same set of implicitly registered public user identities, and are linked to the same service profile, and are considered to have the exact same service configuration for each and every service.

NOTE 1: The S-CSCF recognizes that a given URI is an alias of another URI using the grouping sent from the HSS (see 3GPP TS 29.228 [14]).

**Globally Routeable SIP URI:** a SIP URI of which the hostname part can be resolved to the IP address of the entry entity of the network responsible for the identity represented by the userpart.

**Initial registration:** The registration procedure for a public user identity initiated by the UE in the absence of any valid registration.

**Registration expiration interval:** An indication on how long a registration is valid, indicated using the Expires header field, or the "expires" header field parameter within the Contact header field, according to the procedures specified in RFC 3261 [26].

**Re-registration:** The registration procedure initiated by the UE to refresh or update an already existing registration for a public user identity.

**Registration of an additional public user identity:** The registration procedure initiated by the UE to explicitly register an additional public user identity during the life time of the registration of another registered public user identity, where both public user identities have the same contact address and P-CSCF.

**Emergency registration:** A special registration that relates to binding of a public user identity to a contact address used for emergency service.

**Initial emergency registration:** An emergency registration that is also an initial registration.

**Emergency reregistration:** An emergency registration that is also a reregistration.

**Back-to-Back User Agent (B2BUA):** As given in RFC 3261 [26]. In addition, for the usage in the IM CN subsystem, a SIP element being able to handle a collection of "n" User Agents (behaving each one as UAC and UAS, according to SIP rules), which are linked by some application logic that is fully independent of the SIP rules.

**UE private IP address:** It is assumed that the NAT device performs network address translation between a private and a public network with the UE located in the private network and the IM CN subsystem in the public network. The UE is assumed to be configured with a private IP address. This address will be denoted as UE private IP address.

**UE public IP address:** The NAT device is assumed to be configured with one (or perhaps more) public address(es). When the UE sends a request towards the public network, the NAT replaces the source address in the IP header of the packet, which contains the UE private IP address, with a public IP address assigned to the NAT. This address will be denoted as UE public IP address.

**Encapsulating UDP header:** For the purpose of performing UDP encapsulation according to RFC 3948 [63A] each IPsec ESP packet is wrapped into an additional UDP header. This header is denoted as Encapsulating UDP header.

**Port\_Uenc:** In most residential scenarios, when the NAT device performs address translation, it also performs translation of the source port found in the transport layer (TCP/UDP) headers. Following RFC 3948 [63A], the UE will use port 4500 as source port in the encapsulating UDP header when sending a packet. This port is translated by the NAT into an arbitrarily chosen port number which is denoted as port\_Uenc.

**Multiple registrations:** An additional capability of the UE, P-CSCF and S-CSCF, such that the UE (as identified by the private user identity and instance-id), can create multiple simultaneous registration bindings (flows), associated with one or more contact addresses, to any public user identity. Without this capability, a new registration from the UE for a public user identity replaces the existing registration binding, rather than merely creating an additional binding.

**IMS flow set:** An IMS flow set is a set of flows as defined in RFC 5626 [92]. The flows in an IMS flow set are determined by a combination of transport protocol, IP addresses, and ports. An IMS flow set is established by a successful IMS registration procedure.

NOTE 2: For IPsec, the ports associated with the flow set include protected client ports and protected server ports as defined in 3GPP TS 33.203 [19] and an IMS flow set is made up of the following four flows:

- Flow 1: (IP address UE, port\_uc) <--> (IP address P-CSCF, port\_ps) over TCP;
- Flow 2: (IP address UE, port\_uc) <--> (IP address P-CSCF, port\_ps) over UDP;
- Flow 3: (IP address UE, port\_us) <--> (IP address P-CSCF, port\_pc) over TCP; and
- Flow 4: (IP address UE, port\_us) <--> (IP address P-CSCF, port\_pc) over UDP.

NOTE 3: For IPsec, according to 3GPP TS 33.203 [19], the P-CSCF can only select among flows 1, 3, or 4 when forwarding requests towards the UE, where flow 1 is only possible in case of TCP connection re-use. According to 3GPP TS 33.203 [19], flow 2 is only used for UE originated requests and corresponding responses. The P-CSCF uses flow 2 to identify the correct IMS flow set.

NOTE 4: An IMS flow set can be considered as a realisation of a logical flow as used in RFC 5626 [92]. But this definition does not depend on any particular definition of a logical flow.

NOTE 5: For TLS, the ports associated with the flow set include a protected client port and a protected server port and an IMS flow set is made up of the following flow:

- (IP address UE, port) <--> (IP address P-CSCF, port) over TCP.

NOTE 6: For SIP digest without TLS, an IMS flow set is as defined in RFC 5626 [92].

**IMS flow token:** A IMS flow token is uniquely associated with a IMS flow set. When forwarding a request destined towards the UE, the P-CSCF selects the flow from the IMS flow set denoted by the IMS flow token as appropriate according to 3GPP TS 33.203 [19] and RFC 3261 [26].

**IP Association:** A mapping at the P-CSCF of a UE's packet source IP address, the "sent-by" parameter in the Via header field, and, conditionally, the port with the identities of the UE. This association corresponds to the IP address check table specified in 3GPP TS 33.203 [19].

**Authorised Resource-Priority header field:** a Resource-Priority header field that is either received from another entity in the trust domain relating to the Resource-Priority header field, or which has been identified as generated by a subscriber known to have such priority privileges for the resource priority namespace and level of priority used within that namespace.

**Temporarily authorised Resource-Priority header field:** a Resource Priority header field that has been temporarily approved by the P-CSCF, the S-CSCF, or an IBCF. Temporarily authorised Resource-Priority header field appears in an INVITE request only, and is applied only in the direction P-CSCF to S-CSCF to AS, S-CSCF to AS, or IBCF to S-CSCF to AS, for the request, and the reverse direction for 1xx responses to that request. Subsequent requests in the same dialog will require an authorised Resource-Priority header field in order to obtain priority privileges. It is only valid when all entities are in the same trust domain for the Resource-Priority header field.

**Network-initiated resource reservation:** A mechanism of resource reservation where the IP-CAN on the behalf of network initiates the resources to the UE.

**P-CSCF restoration procedures:** the procedures for the IP-CAN and the UE to handle P-CSCF service interruption scenarios (see 3GPP TS 23.380 [7D]).

**Public network traffic:** traffic sent to the IM CN subsystem for processing according to normal rules of the NGN. This type of traffic is known as public network traffic.

**Private network traffic:** traffic sent to the IM CN subsystem for processing according to an agreed set of rules specific to an enterprise. This type of traffic is known as private network traffic. Private network traffic is normally within a single enterprise, but private network traffic can also exist between two different enterprises if not precluded for regulatory reasons.

NOTE 7: An IP-PBX or application functionality within the IM CN subsystem can change private network traffic to public network traffic and vice versa, by functionality known as "breakout" or "breakin" to the private network. As such a SIP transaction can be variously private network traffic and public network traffic on different hops across a SIP network.

**Privileged sender:** A privileged sender is allowed to send SIP messages where the identities in P-Asserted-Identity will be passed on in the P-CSCF and are not subject to further processing in the P-CSCF.

**S-CSCF restoration procedures:** the procedures for the IM CN subsystem and the UE to handle S-CSCF service interruption scenarios (see 3GPP TS 23.380 [7D]).

**Loopback routing:** A method of routing a SIP request back to the visited network for local breakout according to the roaming architecture for voice over IMS with local breakout as specified in 3GPP TS 23.228 [7].

**Canonical form of a SIP URI:** Canonical form of a SIP URI takes the form "sip:username@domain" as specified in RFC 3261 [26] subclause 10.3. SIP URI comparisons are performed as defined in RFC 3261 [26] subclause 19.1.4.

For the purposes of the present document, the following terms and definitions given in RFC 1594 [20B] apply.

#### **Fully-Qualified Domain Name (FQDN)**

For the purposes of the present document, the following terms and definitions given in RFC 3261 [26] apply (unless otherwise specified see clause 6).

**Client**  
**Dialog**  
**Final response**  
**Header**  
**Header field**  
**Loose routing**  
**Method**  
**Option-tag** (see RFC 3261 [26] subclause 19.2)  
**Provisional response**  
**Proxy, proxy server**  
**Recursion**  
**Redirect server**  
**Registrar**  
**Request**  
**Response**  
**Server**  
**Session**  
**(SIP) transaction**  
**Stateful proxy**  
**Stateless proxy**  
**Status-code** (see RFC 3261 [26] subclause 7.2)  
**Tag** (see RFC 3261 [26] subclause 19.3)  
**Target Refresh Request**  
**User agent client (UAC)**  
**User agent server (UAS)**  
**User agent (UA)**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [2] subclause 4.1.1.1 and subclause 4a.7 apply:

**3GPP AAA proxy**  
**3GPP AAA server**

**Breakout Gateway Control Function (BGCF)**  
**Call Session Control Function (CSCF)**  
**Home Subscriber Server (HSS)**  
**Location Retrieval Function (LRF)**  
**Media Gateway Control Function (MGCF)**  
**MSC Server enhanced for IMS centralized services**  
**Multimedia Resource Function Processor (MRFP)**  
**Packet Data Gateway (PDG)**  
**Subscription Locator Function (SLF)**  
**WLAN UE**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.122 [4C] apply:

**Home PLMN (HPLMN)**  
**Visited PLMN (VPLMN)**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.218 [5] subclauses 3.1, 8 and 13 apply:

**Filter criteria**  
**Initial filter criteria**  
**Initial request**  
**ISC gateway function**  
**Media Resource Broker (MRB)**  
**Multimedia Resource Function Controller (MRFC)**  
**Standalone transaction**  
**Subsequent request**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [7] subclauses 3.1, 4.3.3.1, 4.3.6, 4.6, 4.13, 4.15a, 5.2, 5.4.12.1 and 5.10 apply:

**Border control concepts**  
**Geo-local service number**  
**Home local service number**  
**Implicit registration set**  
**Interconnection Border Control Function (IBCF)**  
**Interrogating-CSCF (I-CSCF)**  
**IMS Application Level Gateway (IMS-ALG)**  
**IMS application reference**  
**IMS Application Reference Identifier (IARI)**  
**IMS communication service**  
**IMS Communication Service Identifier (ICSI)**  
**Local service number**  
**IP-Connectivity Access Network (IP-CAN)**  
**Policy and Charging Rule Function (PCRF)**  
**Private user identity**  
**Proxy-CSCF (P-CSCF)**  
**Public Service Identity (PSI)**  
**Public user identity**  
**Roaming Architecture for Voice over IMS with Local Breakout**  
**Serving-CSCF (S-CSCF)**  
**Statically pre-configured PSI**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.292 [7C] apply:

**ICS UE**  
**SCC AS**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.167 [4B] apply:

**Emergency-CSCF (E-CSCF)**  
**Geographical location information**  
**Location identifier**  
**Location information**

For the purposes of the present document, the following terms and definitions given in 3GPP TR 33.203 [19] apply:

**GPRS-IMS-Bundled Authentication (GIBA)**

**Port\_pc**

**Port\_ps**

**Port\_uc**

**Port\_us**

**Protected server port**

**Protected client port**

For the purposes of the present document, the following terms and definitions given in 3GPP TR 21.905 [1] apply:

**IMS Credentials (IMC)**

**International Mobile Equipment Identity (IMEI)**

**IMS SIM (ISIM)**

**Serial Number (SNR)**

**Type Approval Code (TAC)**

**Universal Integrated Circuit Card (UICC)**

**Universal Subscriber Identity Module (USIM)**

**User Equipment (UE)**

For the purposes of the present document, the following terms and definitions given in RFC 2401 [20A] Appendix A apply:

**Security association**

A number of different security associations exist within the IM CN subsystem and within the underlying access transport. Within this document this term specifically applies to either:

- i) the security association that exists between the UE and the P-CSCF. For this usage of the term, the term "security association" only applies to IPsec. This is the only security association that has direct impact on SIP; or
- ii) the security association that exists between the WLAN UE and the PDG. This is the security association that is relevant to the discussion of Interworking WLAN as the underlying IP-CAN.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.234 [7A] apply.

**Interworking WLAN**

For the purposes of the present document, the following terms and definitions given in ITU-T E.164 [57] apply:

**International public telecommunication number**

For the purposes of the present document, the following terms and definitions given in RFC 5012 [91] apply:

**Emergency service identifier**

**Emergency service URN**

**Public Safety Answering Point (PSAP)**

**PSAP URI**

For the purposes of the present document, the following terms and definitions given in RFC 5627 [93] apply:

**Globally Routable User Agent URI (GRUU)**

For the purposes of the present document, the following terms and definitions given in RFC 5626 [92] apply:

**Flow**

For the purposes of the present document, the following terms and definitions given in RFC 4346 [122] appendix B apply:

**TLS session**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.292 [80] apply:

**CS media**



For the purposes of the present document, the following terms and definitions given in 3GPP TS 24.301 [8J] apply:

**IMS Voice over PS Session (IMSVoPS) indicator**  
**Persistent EPS bearer context**

For the purposes of the present document, the following terms and definitions given in 3GPP TS 33.328 [19C] apply:

**End-to-access edge security**

For the purposes of the present document, the following terms and definitions given in 3GPP2 S.R0048-A v4.0 [86F] apply:

**Mobile Equipment Identity (MEID)**  
**Manufacturer code**  
**Serial number**

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

|               |   |
|---------------|---|
| 1xx           | A status-code in the range 101 through 199, and excluding 100 |
| 2xx           | A status-code in the range 200 through 299                    |
| AAA           | Authentication, Authorization and Accounting                  |
| APN           | Access Point Name   |
| AS            | Application Server  |
| ATCF          | Access Transfer Control Function                              |
| AUTN          | Authentication Token  |
| AVP           | Attribute-Value Pair  |
| B2BUA         | Back-to-Back User Agent                                       |
| BGCF          | Breakout Gateway Control Function                             |
| c             | conditional   |
| BRAS          | Broadband Remote Access Server                                |
| CCF           | Charging Collection Function                                  |
| CDF           | Charging Data Function  |
| CDR           | Charging Data Record  |
| CK            | Ciphering Key   |
| CN            | Core Network  |
| CPC           | Calling Party's Category                                      |
| CSCF          | Call Session Control Function                                 |
| DHCP          | Dynamic Host Configuration Protocol                           |
| DNS           | Domain Name System  |
| DOCSIS        | Data Over Cable Service Interface Specification               |
| DTD           | Document Type Definition                                      |
| DTMF          | Dual Tone Multi Frequency                                     |
| DVB           | Digital Video Broadcast                                       |
| DVB-RCS2      | Second Generation DVB Interactive Satellite System            |
| e2ae-security | End-to-access edge security                                   |
| EATF          | Emergency Access Transfer Function                            |
| EC            | Emergency Centre  |
| ECF           | Event Charging Function                                       |
| ECI           | E-UTRAN Cell Identity   |
| ECN           | Explicit Congestion Notification                              |
| E-CSCF        | Emergency CSCF  |
| EF            | Elementary File   |
| EPS           | Evolved Packet System   |
| FAP           | cdma2000 <sup>®</sup> 1x Femtocell Access Point               |
| FQDN          | Fully Qualified Domain Name                                   |
| GCID          | GPRS Charging Identifier                                      |
| GGSN          | Gateway GPRS Support Node                                     |
| GPON          | Gigabit-capable Passive Optical Networks                      |
| GPRS          | General Packet Radio Service                                  |
| GRUU          | Globally Routable User agent URI                              |
| GSTN          | General Switched Telephone Network                            |

|         |  |
|---------|--|
| HPLMN   | Home PLMN                                |
| HSS     | Home Subscriber Server                   |
| HTTP    | HyperText Transfer Protocol              |
| i       | irrelevant                               |
| IARI    | IMS Application Reference Identifier     |
| IBCF    | Interconnection Border Control Function  |
| ICE     | Interactive Connectivity Establishment   |
| I-CSCF  | Interrogating CSCF                       |
| ICS     | Implementation Conformance Statement     |
| ICID    | IM CN subsystem Charging Identifier      |
| ICSI    | IMS Communication Service Identifier     |
| ID      | Identifier                               |
| IK      | Integrity Key                            |
| IM      | IP Multimedia                            |
| IMC     | IMS Credentials                          |
| IMEI    | International Mobile Equipment Identity  |
| IMS     | IP Multimedia core network Subsystem     |
| IMS-AGW | IMS Access Gateway                       |
| IMS-ALG | IMS Application Level Gateway            |
| IMSI    | International Mobile Subscriber Identity |
| IMSVoPS | IMS Voice over PS Session                |
| IOI     | Inter Operator Identifier                |
| IP      | Internet Protocol                        |
| IP-CAN  | IP-Connectivity Access Network           |
| IPsec   | IP security                              |
| IPv4    | Internet Protocol version 4              |
| IPv6    | Internet Protocol version 6              |
| ISC     | IP Multimedia Subsystem Service Control  |
| ISIM    | IM Subscriber Identity Module            |
| I-WLAN  | Interworking – WLAN                      |
| IWF     | Interworking Function                    |
| KMS     | Key Management Service                   |
| LRF     | Location Retrieval Function              |
| m       | mandatory                                |
| MAC     | Message Authentication Code              |
| MCC     | Mobile Country Code                      |
| MEID    | Mobile Equipment IDentity                |
| MGCF    | Media Gateway Control Function           |
| MGW     | Media Gateway                            |
| MNC     | Mobile Network Code                      |
| MRB     | Media Resource Broker                    |
| MRFC    | Multimedia Resource Function Controller  |
| MRFP    | Multimedia Resource Function Processor   |
| MSC     | Mobile-services Switching Centre         |
| n/a     | not applicable                           |
| NAI     | Network Access Identifier                |
| NA(P)T  | Network Address (and Port) Translation   |
| NASS    | Network Attachment Subsystem             |
| NAT     | Network Address Translation              |
| NCC     | Network Control Center                   |
| NCC_ID  | Network Control Center Identifier        |
| NP      | Number Portability                       |
| o       | optional                                 |
| OCF     | Online Charging Function                 |
| OLI     | Originating Line Information             |
| OMR     | Optimal Media Routeing                   |
| PCRF    | Policy and Charging Rules Function       |
| P-CSCF  | Proxy CSCF                               |
| PDG     | Packet Data Gateway                      |
| PDN     | Packet Data Network                      |
| PDP     | Packet Data Protocol                     |
| PDU     | Protocol Data Unit                       |

|         |  |
|---------|--|
| P-GW    | PDN Gateway  |
| PICS    | Protocol Implementation Conformance Statement                        |
| PIDF-LO | Presence Information Data Format Location Object                     |
| PLMN    | Public Land Mobile Network   |
| PSAP    | Public Safety Answering Point  |
| PSI     | Public Service Identity  |
| PSTN    | Public Switched Telephone Network                                    |
| QCI     | QoS Class Identifier   |
| QoS     | Quality of Service   |
| RAND    | RANDom challenge   |
| RCS     | Return Channel via Satellite   |
| RCST    | Return Channel via Satellite Terminal                                |
| RES     | RESponse   |
| RTCP    | Real-time Transport Control Protocol                                 |
| RTP     | Real-time Transport Protocol   |
| SAC     | Service Area Code  |
| SAI     | Service Area Identifier  |
| S-CSCF  | Serving CSCF   |
| SCTP    | Stream Control Transmission Protocol                                 |
| SDES    | Session Description Protocol Security Descriptions for Media Streams |
| SDP     | Session Description Protocol   |
| SDU     | Service Data Unit  |
| SIP     | Session Initiation Protocol  |
| SLF     | Subscription Locator Function  |
| SNR     | Serial Number  |
| SQN     | SeQuence Number  |
| STUN    | Session Traversal Utilities for NAT                                  |
| SVN     | Satellite Virtual Network  |
| SVN-MAC | SVN Medium Access Control label                                      |
| TAC     | Type Approval Code   |
| TFT     | Traffic Flow Template  |
| TURN    | Traversal Using Relay NAT  |
| TLS     | Transport Layer Security   |
| TRF     | Transit and Roaming Function   |
| UA      | User Agent   |
| UAC     | User Agent Client  |
| UAS     | User Agent Server  |
| UDVM    | Universal Decompressor Virtual Machine                               |
| UE      | User Equipment   |
| UICC    | Universal Integrated Circuit Card                                    |
| URI     | Uniform Resource Identifier  |
| URL     | Uniform Resource Locator   |
| URN     | Uniform Resource Name  |
| USAT    | Universal Subscriber Identity Module Application Toolkit             |
| USIM    | Universal Subscriber Identity Module                                 |
| VPLMN   | Visited PLMN   |
| WLAN    | Wireless Local Area Network  |
| x       | prohibited   |
| xDSL    | Digital Subscriber Line (all types)                                  |
| XGPON1  | 10 Gigabit-capable Passive Optical Networks                          |
| XMAC    | expected MAC   |
| XML     | eXtensible Markup Language   |

---

## 3A Interoperability with different IP-CAN

The IM CN subsystem can be accessed by UEs resident in different types of IP-CAN. The main body of this document, and annex A, are general to UEs and IM CN subsystems that are accessed using any type of IP-CAN. Requirements that are dependent on the type of IP-CAN are covered in annexes B, D, E, H, L, M, O, Q, R and S.

At any given time, for a given SIP transaction or dialog, the UE sees only one type of IP-CAN, as reported to it by the lower layers. The UE follows the procedures of the IP-CAN specific annex related to the last type of IP-CAN reported,

even if it is different to one used previously. In particular, handover at the radio layers between two different access technologies can result in such a change while the dialog or transaction proceeds.

At any given time, for a given SIP transaction or dialog, the P-CSCF sees only one type of IP-CAN, as determined by interface to a particular resource architecture, e.g. policy and charging control, and by the access technology reported to it over that interface, or in the absence of this, by preconfiguration in the system. The P-CSCF follows the procedures of the IP-CAN specific annex related to the last type of IP-CAN determined, even if it is different to one used previously. In particular, handover at the radio layers between two different access technologies can result in such a change while the dialog or transaction proceeds.

It is the responsibility of the IP-CAN to ensure that usage of different bearer resources are synchronised on the handover from one IP-CAN to another, e.g. so that a signalling bearer provided by one IP-CAN is a signalling bearer (if provided by that IP-CAN) after handover, and that the appropriate QoS and resource reservation exists after handover. There is no SIP signalling associated with handover at the IP-CAN, and therefore no change in SIP state at one entity is signalled to the peer SIP entity when handover occurs.

In particular the following constraints exist that can have an impact on P-CSCF usage:

- 1) some IP-CANs can explicitly label a bearer as a signalling bearer, while others provide a bearer that has appropriate QoS, but no explicit labelling. Therefore if handover occurs from an IP-CAN with explicit labelling, to an IP-CAN with no explicit labelling, and then back to an IP-CAN with explicit labelling, the signalling will then be on a bearer that is not explicitly labelled; and
- 2) some IP-CANs support signalling of grouping of media within particular bearers, while others do not. Therefore if handover occurs from an IP-CAN with grouping, to an IP-CAN with no grouping, and then back to an IP-CAN with grouping, the signalled grouping can have been lost.

When a UE supports multiple IP-CANs, but does not support handover between those IP-CANs, the annex specific to that IP-CAN applies unmodified.

Where handover between IP-CANs occurs without a reregistration in the IM CN subsystem, the same identities and security credentials for access to the IM CN subsystem are used before and after the handover.

At the P-CSCF, the access technology can variously use the PCRF or NASS in support of both signalling and media bearer provision (or indeed use neither). How to determine which applies is up to network dependent rules, but can be specific to the access technology used by each different UE. Not all access technologies are defined for use with NASS, and not all access technologies are defined for use with the PCRF.

---

## 4 General

### 4.1 Conformance of IM CN subsystem entities to SIP, SDP and other protocols

SIP defines a number of roles which entities can implement in order to support capabilities. These roles are defined in annex A.

Each IM CN subsystem functional entity using an interface at the Gm reference point, the Ma reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Ml reference point, the Mm reference point, the Mr reference point, the Mr' reference point, the Cr reference point, the Mw reference point, the I2 reference point, the I4 reference point and the Ici reference point, and also using the IP multimedia Subsystem Service Control (ISC) Interface, shall implement SIP, as defined by the referenced specifications in Annex A, and in accordance with the constraints and provisions specified in annex A, according to the following roles.

Each IM CN subsystem entity using an interface at the Rc reference point shall implement HTTP as defined in RFC 2616 [196].

The Gm reference point, the Ma reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Ml reference point, the Mm reference point, the Mr reference point, the Mw reference point, the Cr reference point, the I2 reference point, the I4 reference point and the ISC reference point are defined in 3GPP TS 23.002 [2]. The Ici reference point is defined in 3GPP TS 23.228 [7]. The Mr' reference point and the Rc reference point are defined in 3GPP TS 23.218 [5].

For SIP:

- The User Equipment (UE) shall provide the User Agent (UA) role, with the exceptions and additional capabilities to SIP as described in subclause 5.1, with the exceptions and additional capabilities to SDP as described in subclause 6.1, and with the exceptions and additional capabilities to SigComp as described in subclause 8.1. The UE shall also provide the access technology specific procedures described in the appropriate access technology specific annex (see subclause 3A and subclause 9.2.2). The UE may include one or several interconnected SIP elements registered as a single logical entity when the UE performs the functions of an external attached network (e.g. an enterprise network). This specification does not place any constraint on the SIP role played by each of the elements as long as the compound entity appears to the IM CM subsystem as a SIP UA with the aforementioned exceptions and additional capabilities except for the modifications defined by the UE performing the functions of an external attached network modifying role in annex A.

NOTE 1: When the UE performs the functions of an external attached network (e.g. an enterprise network), the internal structure of this UE is outside the scope of this specification. It is expected that in the most common case, several SIP elements will be connected to an additional element directly attached to the IM CN subsystem.

- The P-CSCF shall provide the proxy role, with the exceptions and additional capabilities to SIP as described in subclause 5.2, with the exceptions and additional capabilities to SDP as described in subclause 6.2, and with the exceptions and additional capabilities to SigComp as described in subclause 8.2. Under certain circumstances, if the P-CSCF provides an application level gateway functionality (IMS-ALG), the P-CSCF shall provide the UA role with the additional capabilities, as follows:

- a) when acting as a subscriber to or the recipient of event information (see subclause 5.2);
- b) when performing P-CSCF initiated dialog-release, even when acting as a proxy for the remainder of the dialog (see subclause 5.2);
- c) when performing NAT traversal procedures (see subclause 6.7.2); and
- d) when performing media plane security procedures (see subclause 5.2).

The P-CSCF shall also provide the access technology specific procedures described in the appropriate access technology specific annex (see subclause 3A and subclause 9.2.2).

- The I-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.3.
- The S-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.4, and with the exceptions and additional capabilities to SDP as described in subclause 6.3. Under certain circumstances as described in subclause 5.4, the S-CSCF shall provide the UA role with the additional capabilities, as follows:
  - a) the S-CSCF shall also act as a registrar. When acting as a registrar, or for the purposes of executing a third-party registration, the S-CSCF shall provide the UA role;
  - b) as the notifier of event information the S-CSCF shall provide the UA role;
  - c) when providing a messaging mechanism by sending the MESSAGE method, the S-CSCF shall provide the UA role; and
  - d) when performing S-CSCF initiated dialog release the S-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.
- The MGCF shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.5, and with the exceptions and additional capabilities to SDP as described in subclause 6.4.
- The BGCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.6.
- The AS, acting as terminating UA, or redirect server (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.1), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.2, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.

- The AS, acting as originating UA (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.2), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.3, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.
- The AS, acting as a SIP proxy (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.3), shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.7.4.
- The AS, performing 3rd party call control (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.4), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.5, and with the exceptions and additional capabilities to SDP as described in subclause 6.6. An AS performing media control of an MRFC shall also support the procedures and methods described in subclause 10.2.

NOTE 2: Subclause 5.7 and its subclauses define only the requirements on the AS that relate to SIP. Other requirements are defined in 3GPP TS 23.218 [5].

- The AS, receiving third-party registration requests, shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.
- The MRFC shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.8, and with the exceptions and additional capabilities to SDP as described in subclause 6.5. The MRFC shall also support the procedures and methods described in subclause 10.3 for media control.
- In inline aware mode, the MRB shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.8A. In inline unaware mode, the MRB shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.8A. The MRB shall also support the procedures and methods described in subclause 10.4 for media control.
- The IBCF shall provide the proxy role, with the exceptions and additional capabilities to SIP as described in subclause 5.10. If the IBCF provides an application level gateway functionality (IMS-ALG), then the IBCF shall provide the UA role, with the exceptions and additional capabilities to SIP as described in subclause 5.10, and with the exceptions and additional capabilities to SDP as described in subclause 6.7. If the IBCF provides screening functionality, then the IBCF may provide the UA role, with the exceptions and additional capabilities to SIP as described in subclause 5.10.
- The E-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.11. Under certain circumstances as described in subclause 5.11, the E-CSCF shall provide the UA role in accordance with RFC 3323 [33], with the additional capabilities, as follows:
  - a) when operator policy (e.g. determined by national regulatory requirements applicable to emergency services) allows user requests for suppression of public user identifiers and location information, then the E-CSCF shall provide the UA role, with the exceptions and additional capabilities to SIP as described in subclause 5.11;
  - b) when performing E-CSCF initiated dialog release the E-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog, e.g. for any of the reasons specified in RFC 6442 [89] or RFC 3323 [33];
  - c) when acting as a notifier for the dialog event package the E-CSCF shall provide the UA role; and
  - d) if operator policy allows any LRF to provide a location by value using the mechanism defined in subclause 5.11.3. the E-CSCF shall provide the UA role.
- The LRF shall provide the UA role.
- The ISC gateway function shall provide the proxy role, with the exceptions and additional capabilities to SIP as described in subclause 5.13. If the ISC gateway function provides an application level gateway functionality (IMS-ALG), then the ISC gateway function shall provide the UA role, with the exceptions and additional capabilities to SIP as described in subclause 5.13, and with the exceptions and additional capabilities to SDP as described in subclause 6.7.
- The MSC Server enhanced for ICS shall provide the UA role, with the exceptions and additional capabilities as described in 3GPP TS 24.292 [80].
- The EATF shall provide the UA role, with the exceptions and additional capabilities as described in 3GPP TS 24.237 [8M].

- The ATCF shall:
  - a) provide the proxy role, with the exceptions and additional capabilities as described in 3GPP TS 24.237 [8M]; and
  - b) provide the UA role, with the exceptions and additional capabilities as described in 3GPP TS 24.237 [8M].

In addition to the roles specified above, the P-CSCF, the I-CSCF, the IBCF, the S-CSCF, the BGCF, the E-CSCF and the ISC gateway function can act as a UA when providing server functionality to return a final response for any of the reasons specified in RFC 3261 [26].

In addition to the roles specified above the S-CSCF, AS and an entity hosting the additional routing capabilities as specified in subclause I.3 can act as a UA when providing either client or server functionality when the event package associated with overload control is deployed.

NOTE 3: Annex A can change the status of requirements in referenced specifications. Particular attention is drawn to table A.4 and table A.162 for capabilities within referenced SIP specifications, and to table A.317 and table A.328 for capabilities within referenced SDP specifications. The remaining tables build on these initial tables.

NOTE 4: The allocated roles defined in this clause are the starting point of the requirements from the IETF SIP specifications, and are then the basis for the description of further requirements. Some of these extra requirements formally change the proxy role into a B2BUA. In all other respects other than those more completely described in subclause 5.2 the P-CSCF implements proxy requirements. Despite being a B2BUA a P-CSCF does not implement UA requirements from the IETF RFCs, except as indicated in this specification, e.g., relating to registration event subscription.

NOTE 5: Except as specified in clause 5 or otherwise permitted in RFC 3261, the functional entities providing the proxy role are intended to be transparent to data within received requests and responses. Therefore these entities do not modify message bodies. If local policy applies to restrict such data being passed on, the functional entity has to assume the UA role and reject a request, or if in a response and where such procedures apply, to pass the response on and then clear the session using the BYE method.

All the above entities are functional entities that could be implemented in a number of different physical platforms coexisting with a number of other functional entities. The implementation shall give priority to transactions at one functional entity, e.g. that of the E-CSCF, over non-emergency transactions at other entities on the same physical implementation. Such priority is similar to the priority within the functional entities themselves specified elsewhere in this document.

Additional routing functionality can be provided to support the ability for the IM CN subsystem to provide transit functionality as specified in Annex I. The additional routing functionality shall assume the proxy role.

## 4.2 URI and address assignments

In order for SIP and SDP to operate, the following prerequisite conditions apply:

- 1) I-CSCFs used in registration are allocated SIP URIs. Other IM CN subsystem entities may be allocated SIP URIs. For example sip:pcscf.home1.net and sip:<impl-specific-info>@pcscf.home1.net are valid SIP URIs. If the user part exists, it is an essential part of the address and shall not be omitted when copying or moving the address. How these addresses are assigned to the logical entities is up to the network operator. For example, a single SIP URI may be assigned to all I-CSCFs, and the load shared between various physical boxes by underlying IP capabilities, or separate SIP URIs may be assigned to each I-CSCF, and the load shared between various physical boxes using DNS SRV capabilities.
- 2) All IM CN subsystem entities are allocated IP addresses. Any IM CN subsystem entities can be allocated IPv4 only, IPv6 only or both IPv4 and IPv6 addresses. For systems providing access to IM CN subsystem using a GPRS IP-CAN or an EPS IP-CAN this is specified in 3GPP TS 23.221 [6] subclause 5.1. For systems providing access to IM CN subsystem using a cdma2000<sup>®</sup> packet data subsystem IP-CAN this is specified in subclause M.2.2.1.
- 3) The subscriber is allocated a private user identity by the home network operator. This private user identity is available to the SIP application within the UE. Depending on the network operator, various arrangements exist within the UE for retaining this information:

- a) where an ISIM is present, within the ISIM, see subclause 5.1.1.1A;
- b) where no ISIM is present but USIM is present, the private user identity is derived (see subclause 5.1.1.1A);
- c) neither ISIM nor USIM is present, but IMC is present, within IMC (see subclause 5.1.1.1B.1);
- d) when neither ISIM nor USIM nor IMC is present, the private user identity is available to the UE via other means (see subclause 5.1.1.1B.2).

NOTE 1: 3GPP TS 33.203 [19] specifies that a UE attached to a 3GPP network has an ISIM or a USIM.

NOTE 2: The SIP URIs can be resolved by using any of public DNSs, private DNSs, or peer-to-peer agreements.

- 4) The subscriber is allocated one or more public user identities by the home network operator. The public user identity shall take the form of SIP URI as specified in RFC 3261 [26] or tel URI as specified in RFC 3966 [22]. At least one of the public user identities is a SIP URI. All registered public user identities are available to the SIP application within the UE, after registration. Depending on the network operator, various arrangements exist within the UE for retaining this information:
  - a) where an ISIM is present, at least one public user identity, which is a SIP URI, within the ISIM, see subclause 5.1.1.1A;
  - b) where no ISIM is present but USIM is present, a temporary public user identity is derived (see subclause 5.1.1.1A);
  - c) neither ISIM nor USIM is present, but IMC is present, within IMC (see subclause 5.1.1.1B.1);
  - d) when neither ISIM nor USIM nor IMC is present, the public user identities are available to the UE via other means (see subclause 5.1.1.1B.2).

NOTE 3: 3GPP TS 33.203 [19] specifies that a UE attached to a 3GPP network has an ISIM or a USIM.

- 5) If the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations, then it shall have an Instance ID, in conformance with the mandatory requirements for Instance IDs specified in RFC 5627 [93] and RFC 5626 [92].
- 6) For each tel URI, there is at least one alias SIP URI in the set of implicitly registered public user identities that is used to implicitly register the associated tel URI.

NOTE 4: For each tel URI, there always exists a SIP URI that has identical user part as the tel URI and the "user" SIP URI parameter equals "phone" (see RFC 3261 [26] subclause 19.1.6), that represents the same public user identity. If a tel URI identifies a subscriber served by the IM CN subsystem, then the hostport parameter of the respective SIP URI contains the home domain name of the IM CN subsystem to which the subscriber belongs.

- 6A) Identification of the UE to a PSAP with point of presence in the CS domain is not possible if a tel URI is not included in the set of implicitly registered public user identities. If the included tel URI is associated either with the first entry in the list of public user identities provisioned in the UE or with the temporary public user identity, then a PSAP can uniquely identify the UE if emergency registration is performed.

NOTE 5: The tel URI uniquely identifies the UE by not sharing any of the implicit registered public user identities in the implicit registration set that contains this tel URI.

NOTE 6: Emergency registration is not always needed or supported.

- 7) The public user identities may be shared across multiple UEs. A particular public user identity may be simultaneously registered from multiple UEs that use different private user identities and different contact addresses. When reregistering and deregistering a given public user identity and associated contact address, the UE will use the same private user identity that it had used during the initial registration of the respective public user identity and associated contact address. If the tel URI is a shared public user identity, then the associated alias SIP URI is also a shared public user identity. Likewise, if the alias SIP URI is a shared public user identity, then the associated tel URI is also a shared public user identity.
- 8) For the purpose of access to the IM CN subsystem, UEs can be allocated IPv4 only, IPv6 only or both IPv4 and IPv6 addresses. For systems providing access to IM CN subsystem using a UMTS/GSM network this is



specified in 3GPP TS 23.221 [6] subclause 5.1 (see subclause 9.2.1 for the assignment procedures). For systems providing access to IM CN subsystem using a cdma2000<sup>®</sup> network this is specified in subclause M.2.2.1.

- 9) For the purpose of indicating an IMS communication service to the network, UEs are assigned ICSI values appropriate to the IMS communication services supported by the UE, coded as URNs as specified in subclause 7.2A.8.2.

NOTE 7: cdma2000<sup>®</sup> is a registered trademark of the Telecommunications Industry Association (TIA-USA).

- 10) E-CSCFs are allocated multiple SIP URIs. The SIP URI configured in the P-CSCF, AS or IBCF to reach the E-CSCF is distinct from the one given by the E-CSCF to the EATF such that EATF can reach the E-CSCF.

- 11) If the UE supports RFC 6140 [191] and performs the functions of an external attached network, the subscriber is allocated one or usually more public user identities by the home network operator. The public user identity(s) shall be allocated as global numbers in the international format.

## 4.2A Transport mechanisms

This document makes no requirement on the transport protocol used to transfer signalling information over and above that specified in RFC 3261 [26] clause 18. However, the UE and IM CN subsystem entities shall transport SIP messages longer than 1300 bytes according to the procedures of RFC 3261 [26] subclause 18.1.1, even if a mechanism exists of discovering a maximum transmission unit size longer than 1500 bytes.

NOTE: Support of SCTP as specified in RFC 4168 [96] is optional for IM CN subsystem entities implementing the role of a UA or proxy. SCTP transport between the UE and P-CSCF is not supported in the present document. Support of the SCTP transport is currently not described in 3GPP TS 33.203 [19].

For initial REGISTER requests, the UE and the P-CSCF shall apply port handling according to subclause 5.1.1.2 and subclause 5.2.2.

The UE and the P-CSCF shall send and receive request and responses other than initial REGISTER requests on the protected ports as described in 3GPP TS 33.203 [19].

In case of an emergency session if the UE does not have sufficient credentials to authenticate with the IM CN subsystem and regulations allow, the UE and P-CSCF shall send request and responses other than initial REGISTER requests on non protected ports.

## 4.2B Security mechanisms

### 4.2B.1 Signalling security

3GPP TS 33.203 [19] defines the security features and mechanisms for secure access to the IM CN subsystem. This document defines a number of access security mechanisms, as summarised in table 4-1.

**Table 4-1: Summary of access security mechanisms to the IM CN subsystem**

| Mechanism  | Authentication          | Integrity protection | Use of security agreement in accordance with RFC 3329 [48] | Support (as defined in 3GPP TS 33.203 [19])  |
|--|-------------------------|----------------------|--|--|
| IMS AKA plus IPsec ESP (see 3GPP TS 33.203 [19] clause 6)  | IMS AKA                 | IPsec ESP            | Yes  | Mandatory for all UEs containing a UICC, else optional. Mandatory for all P-CSCF, I-CSCF, S-CSCF |
| SIP digest plus check of IP association (see 3GPP TS 33.203 [19] annex N) (note 2)   | SIP digest              | None (note 3)        | No   | Optional for UEs<br>Optional for P-CSCF, I-CSCF, S-CSCF  |
| SIP digest plus Proxy Authentication (see 3GPP TS 33.203 [19] annex N) (note 2)  | SIP digest              | None (note 3)        | No   | Optional for UEs<br>Optional for P-CSCF, I-CSCF, S-CSCF  |
| SIP digest with TLS (see 3GPP TS 33.203 [19] annex N and annex O)  | SIP digest              | TLS session          | Yes  | Optional for UEs<br>Optional for P-CSCF, I-CSCF, S-CSCF  |
| NASS-IMS bundled authentication (see 3GPP TS 33.203 [19] annex R) (notes 4, 5)   | not applicable (note 1) | None (note 3)        | No   | No UE support required<br>Optional for P-CSCF, I-CSCF, S-CSCF                                    |
| GPRS-IMS-Bundled authentication (see 3GPP TS 33.203 [19] annex S) (note 5)   | not applicable (note 1) | None (note 3)        | No   | Optional for UEs<br>Optional for P-CSCF, I-CSCF, S-CSCF  |
| Trusted node authentication (see 3GPP TS 33.203 [19] annex U)  | not applicable (note 6) | None (note 3)        | No   | No UE support required<br>Optional for I-CSCF, S-CSCF  |
| <p>NOTE 1: Authentication is not provided as part of the IM CN subsystem signalling.</p> <p>NOTE 2: The term "SIP digest without TLS" is used in this specification to refer to both "SIP digest plus check of IP association" and "SIP digest plus Proxy Authentication".</p> <p>NOTE 3: This security mechanism does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure.</p> <p>NOTE 4: A P-Access-Network-Info aware P-CSCF is required in order to provide NASS-IMS bundled authentication.</p> <p>NOTE 5: The P-CSCF is restricted to the home network when performing this security mechanism.</p> <p>NOTE 6: Trusted node authentication. For example the MSC server enhanced for IMS centralized services has authenticated the UE and as a consequence S-CSCF will skip authentication.</p> |                         |                      |  |  |

Specification of the mechanisms identified within table 4-1 within this document are provided in clause 5. Subclauses where security procedures are required consist of a general subclause applicable whichever security mechanisms are in use, and a separate subclause for each security mechanism identified by a row within table 4-1.

TLS is optional to implement and is used only in combination with SIP digest authentication. Authentication associated with registration to the IM CN subsystem is applicable to IMS AKA and SIP digest and is covered in subclause 5.1.1 for the UE, subclause 5.2.2 for the P-CSCF and subclause 5.4.1 for the S-CSCF. Additionally, SIP digest allows for authentication to also occur on an initial request for a dialog or a request for a standalone transaction, this additional capability is covered in subclause 5.1.2A and subclause 5.4.3.2.

If a UE that implements SIP digest is configured not to use TLS, then the UE does not establish a TLS session toward the P-CSCF. If a UE supports TLS, then the UE supports TLS as described in 3GPP TS 33.203 [19].

For SIP digest authentication, the P-CSCF can be configured to have TLS required or disabled:

- if TLS is required, the P-CSCF requires the establishment of a TLS session from all SIP digest UEs, in order to access IMS subsequent to registration; or

- if TLS is disabled, the P-CSCF does not allow the establishment of a TLS session from any UE.

NOTE: The mechanism to configure the P-CSCF to have TLS required or disabled is outside the scope of this specification.

SIP digest cannot be used in conjunction with the procedures of Annex F.

For emergency calls, 3GPP TS 33.203 [19] specifies some relaxations, which are further described in the subclauses of this document relating to emergency calls.

3GPP TS 33.210 [19A] defines the security architecture for network domain IP based control planes.

3GPP TS 33.210 [19A] applies for security mechanisms between entities in the IM CN subsystem.

## 4.2B.2 Media security

3GPP TS 33.328 [19C] defines mechanisms for support of security on the media plane.

This document defines the required elements for signalling the support of media security.

The media security mechanisms are summarised as shown in table 4-2.

**Table 4-2: Summary of media security mechanisms to the IM CN subsystem**

| Mechanism   | Applicable to media   | Support required by UE   | Support required by IM CN subsystem entities  | Network support outside IM CN subsystem entities |
|---|-----------------------|--|---|--|
| End-to-access-edge media security using SDES.   | RTP based media only. | Support RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/34, A.317/36 and A.317/37. | P-CSCF (IMS-ALG) is required. P-CSCF support of RFC 3329 additions specified in subclause 7.2A.7 and SDP extensions specified in table A.317, items A.317/34, A.317/36 and A.317/37. (NOTE) | Not applicable.                                  |
| End-to-end media security using SDES.   | RTP based media only. | Support SDP extensions specified in table A.317, items A.317/34 and A.317/36.  | Not applicable.   | Not applicable.                                  |
| End-to-end media security using KMS.  | RTP based media only. | Support SDP extensions specified in table A.317, items A.317/34 and A.317/35.  | Not applicable.   | GBA and KMS support required.                    |
| NOTE: Support of end-to-access-edge security is determined entirely by the network operator of the P-CSCF, which need not be the same network operator as that of the S-CSCF. |                       |  |   |  |

For media security, the UE supports the SDES key management protocol and optionally the KMS key management protocol as defined in 3GPP TS 33.328 [19C] and SRTP as defined in RFC 3711 [169] for secure transport of media.

There is no support for media security in the MGCF, because there would be no end-to-end security support on calls interworked with the CS domain and the CS user. In this release of this document, there is no support for media security in the MRF. End-to-access-edge security is not impacted by this absence of support.

For emergency calls, it is not expected that PSAPs would support end-to-end media security and therefore the procedures of this document do not allow the UE to establish such sessions with end-to-end security. End-to-access-edge media security is not impacted and can be used on emergency calls.

When the UE performs the functions of an external attached network (e.g. an enterprise network):

- where end-to-access-edge security is used, the UE functionality is expected to be in the gateway of the external attached network, and support for further media security is outside the scope of this document; and

- where end-to-end security is used, the UE functionality is expected to be supported by the endpoints in the attached network.

## 4.3 Routing principles of IM CN subsystem entities

Each IM CN subsystem functional entity shall apply loose routing policy as described in RFC 3261 [26], when processing a SIP request. In cases where the I-CSCF, IBCF, S-CSCF and the E-CSCF may interact with strict routers in non IM CN subsystem networks, the I-CSCF, IBCF, S-CSCF and E-CSCF shall use the routing procedures defined in RFC 3261 [26] to ensure interoperability with strict routers.

## 4.4 Trust domain

### 4.4.1 General

RFC 3325 [34] provides for the existence and trust of an asserted identity within a trust domain. For the IM CN subsystem, this trust domain consists of the functional entities that belong to the same operator's network (P-CSCF, the E-CSCF, the I-CSCF, the IBCF, the S-CSCF, the BGCF, the MGCF, the MRFC, the MRB, the EATF, the ATCF, the ISC gateway function, and all ASs that are included in the trust domain). Additionally, other nodes within the IM CN subsystem that are not part of the same operator's domain may or may not be part of the trust domain, depending on whether an interconnect agreement exists with the remote network. SIP functional entities that belong to a network for which there is an interconnect agreement are part of the trust domain. ASs outside the operator's network can also belong to the trust domain if they have a trusted relationship with the home network.

NOTE 1: Whether any peer functional entity is regarded as part of the same operator's domain, and therefore part of the same trust domain, is dependent on operator policy which is preconfigured into each functional entity.

NOTE 2: For the purpose of this document, the PSAP is typically regarded as being within the trust domain, except where indicated. National regulator policy applicable to emergency services determines the trust domain applicable to certain header fields. This means that e.g. the handling of the P-Access-Network-Info header field, P-Asserted-Identity header field and the History-Info header field can be as if the PSAP is within the trust domain, and trust domain issues will be resolved accordingly.

Within the IM CN subsystem trust domains will be applied to a number of header fields. These trust domains do not necessarily contain the same functional entities or cover the same operator domains. The procedures in this subclause apply to the functional entities in clause 5 in the case where a trust domain boundary exists at that functional entity.

Where the IM CN subsystem supports business communication, different trust domains can apply to public network traffic, and to private network traffic belonging to each supported corporate network.

NOTE 3: Where an external attached network (e.g. an enterprise network) is in use, the edges of the trust domains need not necessarily lie at the P-CSCF. In this release of the specification, the means by which the P-CSCF learns of such attached devices, and therefore different trust domain requirements to apply, is not provided in the specification and is assumed to be by configuration or by a mechanism outside the scope of this release of the specification.

A trust domain applies for the purpose of the following header fields: P-Asserted-Identity, P-Access-Network-Info, History-Info, Resource-Priority, P-Asserted-Service, Reason (only in a response), P-Profile-Key, P-Private-Network-Indication, P-Served-User, P-Early-Media and Feature-Caps. A trust domain applies for the purpose of the CPC and OLI tel URI parameters. The trust domains of these header fields and parameters need not have the same boundaries. Clause 5 defines additional procedures concerning these header fields.

### 4.4.2 P-Asserted-Identity

A functional entity at the boundary of the trust domain will need to determine whether to remove the P-Asserted-Identity header field according to RFC 3325 [34] when SIP signalling crosses the boundary of the trust domain. The priv-value "id" shall not be removed from the Privacy header field when SIP signalling crosses the boundary of the trust domain. Subclause 5.4 identifies additional cases for the removal of the P-Asserted-Identity header field.

### 4.4.3 P-Access-Network-Info

A functional entity at the boundary of the trust domain shall remove any P-Access-Network-Info header field in accordance with RFC 7315 [52].

#### 4.4.4 History-Info

A functional entity at the boundary of the trust domain will need to determine whether to remove the History-Info header field according to RFC 4244 [66] subclause 3.3 when SIP signalling crosses the boundary of the trust domain. Subclause 5.4 identifies additional cases for the removal of the History-Info header field.

#### 4.4.5 P-Asserted-Service

A functional entity at the boundary of the trust domain will need to determine whether to remove the P-Asserted-Service header field according to RFC 6050 [121] when SIP signalling crosses the boundary of the trust domain.

#### 4.4.6 Resource-Priority

A functional entity shall only include a Resource-Priority header field in a request or response forwarded to another entity within the trust domain. If a request or response is forwarded to an entity outside the trust domain, the functional entity shall remove the Resource-Priority header field from the forwarded request or response. If a request or response is received from an untrusted entity (with the exception requests or responses received by the P-CSCF from the UE for which procedures are defined in subclause 5.2) that contains the Resource-Priority header field, the functional entity shall remove the Resource-Priority header field before forwarding the request or response within the trust domain.

NOTE: Alternate treatments can be applied when a non-trusted Resource-Priority header field is received over the boundary of trust domain. The exact treatment (e.g. removal, modification, or passing of the Resource-Priority header field) is left to national regulation and network configuration.

#### 4.4.7 Reason (in a response)

A functional entity shall only include a Reason header field in a response forwarded to another entity within the trust domain (as specified in RFC 6432 [130]). If a response is forwarded to an entity outside the trust domain, the functional entity shall remove the Reason header field from the forwarded response.

NOTE: A Reason header field can be received in a response from outside the trust domain and will not be removed.

#### 4.4.8 P-Profile-Key

A functional entity at the boundary of the trust domain will need to determine whether to remove the P-Profile-Key header field as defined in RFC 5002 [97] when SIP signalling crosses the boundary of the trust domain.

#### 4.4.9 P-Served-User

A functional entity at the boundary of the trust domain will need to determine whether to remove the P-Served-User header field according to RFC 5502 [133] when SIP signalling crosses the boundary of the trust domain.

#### 4.4.10 P-Private-Network-Indication

A functional entity shall only include a P-Private-Network-Indication header field in a request forwarded to another entity within the trust domain. If a request is forwarded to an entity outside the trust domain, the functional entity shall remove the P-Private-Network-Indication header field from the forwarded request. If a request is received from an untrusted entity that contains the P-Private-Network-Indication header field, the functional entity shall remove the P-Private-Network-Indication header field before forwarding the request within the trust domain.

NOTE 1: Other entities within the enterprise will frequently be part of this trust domain.

NOTE 2: The presence of the P-Private-Network-Indication header field is an indication that the request constitutes private network traffic. This can modify the trust domain behaviour for other header fields.

NOTE 3: If a trust domain boundary is encountered for this header field without appropriate business communication processing, then this can be an indication that misconfiguration has occurred in the IM CN subsystem. Removal of this header field changes the request from private network traffic to public network traffic.

### 4.4.11 P-Early-Media

A functional entity at the boundary of the trust domain will need to determine whether to remove the P-Early-Media header field as defined in RFC 5009 [109] when SIP signalling crosses the boundary of the trust domain.

### 4.4.12 CPC and OLI

Entities in the IM CN subsystem shall restrict "cpc" and "oli" URI parameters to specific domains that are trusted and support the "cpc" and "oli" URI parameters. Therefore for the purpose of the "cpc" and "oli" URI parameters within this specification, a trust domain also applies.

SIP functional entities within the trust domain shall remove the "cpc" and "oli" URI parameters when the SIP signalling crosses the boundary of the trust domain.

### 4.4.13 Feature-Caps

A functional entity at the boundary of the trust domain shall remove all Feature-Caps header fields received from UEs and external networks outside the trust domain.

NOTE: A UE that is a privileged sender is considered as part of the trust domain.

## 4.5 Charging correlation principles for IM CN subsystems

### 4.5.1 Overview

This subclause describes charging correlation principles to aid with the readability of charging related procedures in clause 5. See 3GPP TS 32.240 [16] and 3GPP TS 32.260 [17] for further information on charging.

The IM CN subsystem generates and retrieves the following charging correlation information for later use with offline and online charging:

1. IM CN subsystem Charging Identifier (ICID);
2. Access network charging information;
3. Inter Operator Identifier (IOI);
4. Charging function addresses:
  - a. Charging Data Function (CDF);
  - b. Online Charging Function (OCF).

How to use and where to generate the parameters in IM CN subsystems are described further in the subclauses that follow. The charging correlation information is encoded in the P-Charging-Vector header field as defined in subclause 7.2A.5. The P-Charging-Vector header field contains the following header field parameters: "icid-value", "related-icid", "access-network-charging-info", "orig-ioi", "term-ioi" and "transit-ioi".

The offline and online charging function addresses are encoded in the P-Charging-Function-Addresses as defined in RFC 7315 [52]. The P-Charging-Function-Addresses header field contains the following header field parameters: "ccf" for CDF and "ecf" for OCF.

NOTE: P-Charging-Function-Addresses parameters were defined using previous terminology.

### 4.5.2 IM CN subsystem charging identifier (ICID)

The ICID is the session level data shared among the IM CN subsystem entities including ASs in both the calling and called IM CN subsystems. The ICID is used also for session unrelated messages (e.g. SUBSCRIBE request, NOTIFY request, MESSAGE request) for the correlation with CDRs generated among the IM CN subsystem entities.

The first IM CN subsystem entity involved in a SIP transaction will generate the ICID and include it in the "icid-value" header field parameter of the P-Charging-Vector header field in the SIP request.

For a dialog relating to a session, the generation of the ICID will be performed only on the initial INVITE request. This ICID will be used for the initial INVITE request, and all subsequent signalling that contains a P-Charging-Vector header field.

For all other transactions, generation of the ICID will occur on each SIP request and be included in that SIP request.

See 3GPP TS 32.260 [17] for requirements on the format of ICID. The P-CSCF will generate an ICID for UE-originated calls. The I-CSCF will generate an ICID for UE-terminated calls if there is no ICID received in the initial request (e.g. the calling party network does not behave as an IM CN subsystem). The AS will generate an ICID when acting as an originating UA. The MGCF will generate an ICID for PSTN/PLMN originated calls. The MSC server will generate an ICID for ICS and SRVCC originated calls. Each entity that processes the SIP request will extract the ICID for possible later use in a CDR. The I-CSCF and S-CSCF are also allowed to generate a new ICID for UE-terminated calls received from another network.

There is also an ICID generated by the P-CSCF with a REGISTER request that is passed in a unique instance of P-Charging-Vector header field. The valid duration of the ICID is specified in 3GPP TS 32.260 [17].

The "icid-value" header field parameter is included in any request that includes the P-Charging-Vector header field. However, the P-Charging-Vector (and ICID) is not passed to the UE.

The ICID is also passed from the P-CSCF to the IP-CAN via PCRF. The interface supporting this operation is outside the scope of this document.

## 4.5.2A Related ICID

During the process of SRVCC access transfer the MSC server or the P-CSCF generates an ICID for the target access leg. For the purpose of charging correlation between the source access leg and the target access leg when the user is roaming the SCC AS and the ATCF includes the ICID used on the source access leg in the "related-icid" header field parameter of the P-Charging-Vector header field returned in 1xx and 2xx responses to the initial INVITE request.

## 4.5.3 Access network charging information

### 4.5.3.1 General

The access network charging information are the media flow level data shared among the IM CN subsystem entities for one side of the session (either the calling or called side). GPRS charging information (GGSN identifier and PDP context information) is an example of access network charging information.

### 4.5.3.2 Access network charging information

The IP-CAN provides the access network charging information to the IM CN subsystem. This information is used to correlate IP-CAN CDRs with IM CN subsystem CDRs, i.e. the access network charging information is used to correlate the bearer level with the session level.

The access network charging information is generated at the first opportunity after the resources are allocated at the IP-CAN. The access network charging information is passed from IP-CAN to P-CSCF via PCRF, over the Rx and Gx interfaces. Access network charging information will be updated with new information during the session as media flows are added or removed. The P-CSCF provides the access network charging information to the S-CSCF. The S-CSCF may also pass the information to an AS, which may be needed for online pre-pay applications. The access network charging information for the originating network is used only within that network, and similarly the access network charging information for the terminating network is used only within that network. Thus the access network charging information are not shared between the calling and called networks. The access network charging information is not passed towards the external ASs from its own network.

The access network charging information is populated in the P-Charging-Vector header field.

The access network charging information can be included in a P-Charging-Vector header field in dialog forming requests, mid-dialog requests, and responses. This is dependant on when updated information is available in the P-CSCF.

## 4.5.4 Inter operator identifier (IOI)

The Inter Operator Identifier (IOI) is a globally unique identifier to share between sending and receiving networks, service providers or content providers.

The sending network populates the "orig-ioi" header field parameter of the P-Charging-Vector header field in a request and thereby identifies the operator network from which the request was sent. The "term-ioi" header field parameter is left out of the P-Charging-Vector header field in this request. The sending network retrieves the "term-ioi" header field parameter from the P-Charging-Vector header field within the message sent in response, which identifies the operator network from which the response was sent.

The receiving network retrieves the "orig-ioi" header field parameter from the P-Charging-Vector header field in the request, which identifies the operator network from which the request was sent. The receiving network populates the "term-ioi" header field parameter of the P-Charging-Vector header field in the response to the request, which identifies the operator network from which the response was sent.

There are three types of IOI:

- a) Type 1 IOI, between the visited network and the home network. This includes the following cases:
- between the P-CSCF (possibly in the visited network) and the S-CSCF in the home network. This is exchanged in REGISTER requests and responses;
  - between the SCC AS in the home network and the ATCF (possible in the visited network). This is exchanged in MESSAGE requests and responses; and

NOTE: For applications where the primary relationship is home and visited network, request and responses to the request will normally contain a type 1 IOI value.

- when using Roaming Architecture for Voice over IMS with Local Breakout and loopback routing occurs, between the S-CSCF of the home network and the TRF of the visited network or between the BGCF of the home network and the TRF of the visited network. This is exchanged in all session-related requests and responses.

- b) Type 2 IOI, between originating network and the terminating network. This includes the following cases:

- between the the S-CSCF of the home originating network and the S-CSCF of the home terminating network or between the S-CSCF of the home originating network and the MGCF when a call/session is terminated at the PSTN/PLMN;
- between the MGCF and the S-CSCF of the home terminating network when a call/session is originated from the PSTN/PLMN or with a PSI AS when accessed across I-CSCF; and
- when using Roaming Architecture for Voice over IMS with Local Breakout and loopback routing occurs, between the TRF of the visited network and the S-CSCF of the home terminating network.

This is exchanged in all session-related and session-unrelated requests and responses.

Additionally, for emergency transactions, a type 2 IOI is exchanged between the E-CSCF and the MGCF or IBCF where the request is routed to a PSAP. In scenarios where the E-CSCF receives emergency requests from an S-CSCF, a type 2 IOI is exchanged. This can also occur where the E-CSCF receives emergency requests from an IBCF.

- c) Type 3 IOI, between the S-CSCF or I-CSCF of the home operator network and any AS. Type 3 IOI are also used between E-CSCF and LRF, between E-CSCF and EATF, and between transit function and AS. The type 3 IOI is exchanged in all session-related and session-unrelated requests and responses.

Each entity that processes the SIP request will extract the IOI for possible later use in a CDR. The valid duration of the IOI is specified in 3GPP TS 32.240 [16].

#### 4.5.4A Transit inter operator identifier (Transit IOI)

The Transit Inter Operator Identifier (Transit IOI) is a globally unique identifier to share between sending, transit and receiving networks, service providers or content providers.

The sending network retrieves the "transit-ioi" header field parameter value(s) from the P-Charging-Vector header field within the message sent in response, which identify the operator network(s) which the response was transitting.

The transit network(s) populate(s) the "transit-ioi" header field parameter value(s) of the P-Charging-Vector header field in a request and thereby identify(ies) the operator network(s) which the request was transitting. The "transit-ioi"



header field parameter is an indexed value that is incremented each time a value is added. When the index is calculated then "void" entries are taken into account.

The transit network(s) populate(s) the "transit-ioi" header field parameter value(s) of the P-Charging-Vector header field in the response to the request and thereby identify(ies) the operator network(s) which the response was transitting. The "transit-ioi" header field parameter is an indexed value that is incremented each time a value is added. When the index is calculated then "void" entries are taken into account.

The receiving network retrieves the "transit-ioi" header field parameter value(s) from the P-Charging-Vector header field in the request, which identify the operator network(s) which the request was transitting.

#### EXAMPLE:

Transit-IOI in a request when arriving on the terminating side:

```
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net; transit-  
ioi="operator_A.1, void, operator_B.3"
```

Transit-IOI in the corresponding response when arriving on the originating side:

```
P-Charging-Vector: icid-value="AyretyU0dm+6O2IrT5tAFrbHLso=023551024"; orig-ioi=home1.net; term-  
ioi=home2.net; "transit-ioi=operator_B.1, void, operator_A.3"
```

The Transit IOI is exchanged between additional routing functions as defined in Annex I and the S-CSCF of the home terminating network, or the additional routing functions as defined in Annex I of the transit network(s) and the S-CSCF of the home originating network, or between the additional routing functions as defined in Annex I and the MGCF when a call/session is terminated at the PSTN/PLMN, or between the MGCF and the S-CSCF of the home terminating network when a call/session was transitting the PSTN/PLMN. This may be exchanged in all session-related and session-unrelated requests and responses. Additional routing functions as defined in Annex I may add or delete "transit-ioi" header field parameter value(s) in the P-Charging-Vector header field in requests and in responses, in accordance with the procedures in 3GPP TS 32.260 [17].

NOTE: Transit IOIs can also be exchanged with non 3GPP networks, e.g. IPX networks.

Each entity that processes the SIP requests and responses may extract the Transit IOI for charging purposes, as described in 3GPP TS 32.260 [17].

## 4.5.5 Charging function addresses

Charging function addresses are distributed to each of the IM CN subsystem entities in the home network for one side of the session (either the calling or called side) and provide a common location for each entity to send charging information. Charging Data Function (CDF) addresses are used for offline billing. Online Charging Function (OCF) addresses are used for online billing.

There may be multiple addresses for CDF and OCF addresses populated into the P-Charging-Function-Addresses header field of the SIP request or response. The header field parameters are "ccf" and "ecf" for CDF and OCF, respectively. At least one instance of either "ccf" or "ecf" header field parameter is required. If "ccf" header field parameter is included for offline charging, then a secondary "ccf" header field parameter may be included by each network for redundancy purposes, but the first instance of "ccf" header field parameter is the primary address. If ecf address is included for online charging, then a secondary instance may also be included for redundancy.

The CDF and/or OCF addresses are retrieved from an Home Subscriber Server (HSS) via the Cx interface and passed by the S-CSCF to subsequent entities. The charging function addresses are passed from the S-CSCF to the IM CN subsystem entities in its home network, but are not passed to the visited network or the UE. When the P-CSCF is allocated in the visited network, then the charging function addresses are obtained by means outside the scope of this document. The AS receives the charging function addresses from the S-CSCF via the ISC interface. CDF and/or OCF addresses may be allocated as locally preconfigured addresses. The AS can also retrieve the charging function address from the HSS via Sh interface.

## 4.5.6 Void

## 4.5.7 Loopback-indication parameter

When there is a desire to send the information that loopback has been applied to an entity, then the loopback-indication parameter is used. This parameter can e.g. be evaluated when processing the P-CSCF CDR and possibly the ATCF CDR to know whether or not to attempt to locate a correlated TRF CDR even for the non-loopback scenario when no such CDR exists. It is used only in accordance with the capabilities specified in this document.

## 4.6 Support of local service numbers

For the IM CN subsystem, the support of local service numbers is provided by an AS in the subscriber's home network as described in subclause 5.7.1.7.

## 4.7 Emergency service

### 4.7.1 Introduction

The need for support of emergency calls in the IM CN subsystem is determined by national regulatory requirements.

### 4.7.2 Emergency calls generated by a UE

If the UE cannot detect the emergency call attempt, the UE initiates the request as per normal procedures as described in subclause 5.1.2A. Depending on network policies, for a non-roaming UE or for a roaming UE where the P-CSCF is in the same network where the UE is roaming an emergency call attempt can succeed even if the UE did not detect that an emergency session is being requested, otherwise the network rejects the request indicating to the UE that the attempt was for an emergency service.

The UE procedures for UE detectable emergency calls are defined in subclause 5.1.6.

The P-CSCF, S-CSCF, and E-CSCF procedures for emergency service are described in subclause 5.2.10, 5.4.8 and 5.11, respectively.

Access dependent aspects of emergency service (e.g. emergency registration support and location provision) are defined in the access technology specific annexes for each access technology.

There are a number of variants within these procedures and which variant gets used depends on a number of issues. These conditions are defined more specifically in 3GPP TS 23.167 [4B] and, where appropriate, in the access technology specific annex, but are summarised as follows:

- a) if the UE knows that it is in its own home network, then an existing registration is permitted to be used for signalling the emergency call, except where item c) applies. The access technology specific annexes define the mechanism by which home network determination is made;
- b) if emergency calls are permitted without security credentials (or additionally where the authentication is not possible or has failed), then the emergency call is made directly without use of any security association created by a registration, and therefore without the registration; and
- c) where the access technology defines emergency bearers for the support of emergency calls, a new emergency registration is required so that these emergency bearers can be used for both signalling and media, unless an existing emergency registration exists on those emergency bearers.

### 4.7.3 Emergency calls generated by an AS

In certain circumstances an AS can identify that a request is an emergency call. This may relate to a request received from a UE (or subscription-based business trunking), or may be a call generated by an AS on behalf of a UE as far as the IM CN subsystem operation is concerned. These applications are outside the scope of this document to define.

Procedures in support of an AS initiating emergency calls are provided in subclause 5.7.1.14.

## 4.7.4 Emergency calls received from an enterprise network

An IBCF can also route emergency calls received from an enterprise network (peering-based business trunking) to an E-CSCF.

## 4.7.5 Location in emergency calls

A number of mechanisms also exist for providing location in support of emergency calls, both for routing to a PSAP, and for use by the PSAP itself, in the IM CN subsystem:

- a) by the inclusion by the UE of the Geolocation header field containing a location by reference or by value (see RFC 6442 [89]);
- b) by the inclusion by the UE of a P-Access-Network-Info header field, which contains a cell identifier or location identifier, which is subsequently mapped, potentially by the recipient, into a real location;
- c) by the inclusion by the P-CSCF of a P-Access-Network-Info header field based on information supplied by either the PCRF or the NASS, and which contains a cell identifier or location identifier, which is subsequently mapped, potentially by the recipient, into a real location;
- d) by the allocation of a location reference that relates to the call by the LRF. Location is then supplied to the recipient over the Le interface (see 3GPP TS 23.167 [4B] for a definition of the Le interface) along with other call information. The LRF can obtain the location from entities outside the IM CN subsystem, e.g. by the e2 interface from the NASS (see ETSI TS 283 035 [98] or from the Gateway Mobile Location Centre (GMLC); and
- e) by the inclusion by the S-CSCF of a P-Access-Network-Info header field based on information supplied by HSS, and which contains a location identifier, which is subsequently mapped, potentially by the recipient, into a real location.

Mechanisms also exist for providing emergency-related information to a PSAP, in requests subsequent to routing an initial request to a PSAP, in the IM CN subsystem:

- a) by the inclusion by the UE of the Geolocation header field containing a location by reference or by value (see RFC 6442 [89]);
- b) by the inclusion by the UE of a P-Access-Network-Info header field, which contains a cell identifier or location identifier, which is subsequently mapped, potentially by the recipient, into a real location;
- c) by the inclusion by the P-CSCF of a P-Access-Network-Info header field based on information supplied by either the PCRF or the NASS, and which contains a cell identifier or location identifier, which is subsequently mapped, potentially by the recipient, into a real location;
- d) by the inclusion by the UE of the emergency-related information as specified in subclause 5.1.6.10; and
- e) by the inclusion by the S-CSCF of a P-Access-Network-Info header field based on information supplied by HSS, and which contains a location identifier, which is subsequently mapped, potentially by the recipient, into a real location.

The E-CSCF routes such a subsequent request to the PSAP using normal SIP procedures. If operator policy determines that an LRF is to be used, this version of the specification does not specify that the emergency-related information in such a subsequent request received by the E-CSCF is provided to the LRF.

NOTE 1: Mechanisms independent from SIP for providing the emergency related information to a PSAP after session setup exist and are not listed. The use of such mechanisms is not precluded.

Which means of providing location is used depends on local regulatory and operator requirements. One or more mechanisms can be used. Location can be subject to privacy constraints.

NOTE 2: A similar variety of mechanisms also exists for normal calls, where location can be made use of by the recipient or by an intermediate AS, again subject to privacy constraints. The LRF is not involved in a normal call, but an AS can obtain location from the e2 interface from the NASS (see ETSI TS 283 035 [98] or from the Gateway Mobile Location Centre (GMLC).

## 4.8 Void

## 4.9 Overlap signalling

### 4.9.1 General

This subclause explains the overlap signalling impacts on the core entities of the IM CN subsystem.

The support of overlap signalling, and each of the overlap signalling method, within the IM CN subsystem, are optional and is dependent on the network policy.

Only one overlap signalling method shall be used within one IM CN subsystem.

NOTE: Interworking between the overlap signalling methods is not specified in this release.

### 4.9.2 Overlap signalling methods

#### 4.9.2.1 In-dialog method

##### 4.9.2.1.1 General

The in-dialog method uses INFO requests or INVITE requests in order to transport additional digits. Before an early dialog has been established, upon reception of a 404 (Not Found) or 484 (Address Incomplete) response to an earlier INVITE request, new INVITE requests will be sent to transfer additional digits (as specified in 3GPP TS 29.163 [11B]). Once an entity establishes an early dialog, by sending a provisional response to a INVITE request, INFO requests will be sent to carry additional digits on the early dialog.

The message body, and associated header values, which is used to carry additional digits in INFO requests is defined in 3GPP TS 29.163 [11B].

#### 4.9.2.2 Multiple-INVITE method

##### 4.9.2.2.1 General

The multiple-INVITE method uses INVITE requests with the same Call ID and From header in order to transport digits (as specified in 3GPP TS 29.163 [11B]).

## 4.9.3 Routeing impacts

### 4.9.3.1 General

If overlap dialing is supported, the IM CN subsystem needs to be configured in such a manner that erroneous routeing of INVITE requests with incomplete numbers towards others entities than the corresponding INVITE requests with full numbers is avoided, for instance towards a default destination for unknown numbers such as a PSTN. Possibly impacted nodes include the S-CSCF for the UE-originated case, the transit routeing function, the I-CSCF, and application servers.

A misrouteing can be avoided by configuring the entity sending overlap signalling in such a manner that it will send the first INVITE request with a sufficient number of digits to find a suitable entry in the translation database. If ENUM is used, the ENUM database in a typical deployment contains sufficient information about the first digits, as required to identify the destination IP domain. Therefore, ENUM is able to handle incomplete numbers in such deployments. As another alternative, the routeing entity can reject calls with unknown numbers with a 404 (Not Found) response, using entries in the routeing database to identify calls towards the PSTN. The S-CSCF for the UE-originated case could also forward calls with unknown numbers to the BGCF, if the BGCF is configured to reject calls to unknown destinations with a 404 (Not Found) response.

### 4.9.3.2 Deterministic routeing

If the multiple-INVITE method is used for overlap signalling, if an entity receives a INVITE request outside an existing dialog with the same Call ID and From header field as a previous INVITE request during a certain period of time, the entity shall route the new INVITE request to the same next hop as the previous INVITE request.

NOTE: INVITE requests with the same Call ID and From header fields received in sequence during a certain period of time belong to the same call. The routing towards the same next hop could be achieved by an appropriately configured database or by the entity comparing the Call ID and From header fields of each INVITE request outside an existing dialog with Call IDs and "tag" From header field parameters of previous INVITE requests. If the entity compares the Call ID and From header field, it stores the information about received Call ID and From header fields at least for a time in the order of call setup times. If paths have been established at registration time, deterministic routing will be automatic for entities on these paths.

### 4.9.3.3 Digit collection

Entities performing routing decisions may require additional digits for a decision where to route an INVITE request. These entities may interact with a routing database to reach this decision.

If no suitable entry in a database is found for the digits received in a INVITE request, an entity can reject the INVITE request with a 404 (Not Found) or 484 (Address Incomplete) response. This method of digit collection can be performed by a SIP proxy and is suitable both for the in-dialog and multiple-INVITE overlap signalling methods. Replying with a 404 (Not Found) response avoids the need to keep apart uncomplete and unknown numbers. The 484 (Address Incomplete) response requires the recognition of incomplete numbers.

NOTE: An HSS does not support the recognition of incomplete numbers. A routing database being queried by ENUM also does not support the recognition of incomplete numbers.

As an alternative for the in-dialogue method, the digit collection function described in annex N.2 may be invoked. It shall be performed by an entity acting as a B2BUA. The digit collection function requires the ability to recognise incomplete number.

## 4.10 Dialog correlation for IM CN subsystems

### 4.10.1 General

The Call-ID header field in combination with the tags in the From header field and in the To header field is the standard mechanism to identify SIP messages which belong to the same dialog. However the Call-ID header field is often changed by B2BUAs and other SIP intermediaries in the end-to-end message path.

To solve this problem, a Session-ID header field containing a globally unique session identifier, as defined in RFC 7329 [162], can be used to correlate SIP messages belonging to the same session. In the case of a concatenation of dialogs, the dialog correlation mechanism indicates that these dialogs belong to the same session.

The usage of the Session-ID header field is specified in annex A.

### 4.10.2 CONF usage

In case of the activation of a 3PTY conference, in the INVITE request to the CONF AS the Session-ID header field is added to the URIs in the URI list, in order to indicate the dialogs which are to be included to the 3PTY conference at the CONF AS, as described in 3GPP TS 24.147 [8B].

## 4.11 Priority mechanisms

In support of priority, the IM CN subsystem uses the mechanisms of RFC 4412 [116]. The request for prioritisation of a transaction / dialog may, for some deployments, be marked with the Resource-Priority header field by the UE. For other deployments, the request is not marked for priority by the UE, but the request is instead identified as a priority request and marked for priority (via a Resource-Priority header field) by a functional entity (e.g., P-CSCF) within the network. Subsequent to successful authorisation at an authorisation point (e.g. AS), request is considered to be authorised.

The characteristics of any priority scheme is defined by the namespace that is used. This determines how priority is applied to the SIP signalling, to the bearer carrying the SIP signalling, and to the bearers carrying any media. Different priority levels exist within each namespace. Priority levels in one namespace have no relationship to the priority levels in any other namespace, i.e. priority level "1" in namespace "A" may have an entirely different level and characteristic of priority treatment to an identically labelled priority level "1" in namespace "B".

A network can support multiple namespaces. It is up to the network operator (potentially based on regulatory or contractual obligations) to define the relationship between the priority mechanisms for each namespace, and indeed

with calls that are not given any priority. It is normal that prioritised calls do not have access to 100% of any available resource and indeed are limited to a much lower figure. Priority is optional, and this document places no requirement on a conformant IM CN subsystem implementation to support priority, or indeed any namespace in a priority scheme. Regulators can however place their own requirements on an operator. Emergency transactions or dialogs (see subclause 4.7) can also have their own priority scheme.

RFC 4412 [116] specifies several resource priority namespaces. For example, certain national MPS implementations use resource priority namespaces of ETS (Emergency Telecommunications Service) and WPS (Wireless Priority Service).

Several ways of using priority exist, depending on the authorisation mechanism adopted. These are identified as follows. In each of these authorisation means authorisation to use the service, the namespace, and the priority level within that namespace:

- 1) Authorisation based on subscription in the IM CN subsystem only, priority requested by the UE using the Resource Priority header field. Whether the user is allowed to use priority or not, and the appropriate namespace and priority levels, is stored as part of the user profile in the HSS. As part of the reg event package subscription, this information is given to the P-CSCF when the contact information for any public user identity changes, and based on this information, the P-CSCF acts as the authorisation point for priority on individual requests. At the P-CSCF, when a Resource-Priority header field is received from the UE, if the requested priority equates to a value (namespace and priority level) that the P-CSCF knows is allowed for that public user identity, the the priority is authorised.
- 2) Authorisation based on a database deployed by an AS; priority requested by the UE using a special dialstring. In this case the user requires no priority subscription information in the HSS. Specific dialstrings are configured in the P-CSCF. When a request is received from the UE by the P-CSCF, if the request contains a specific dialstring that is recognised by the P-CSCF as being eligible for priority treatment, the request is marked for temporary priority, subject to subsequent authorisation by an authorisation point (i.e., AS). And all such requests are routed to an AS. Final authorisation is granted by the AS, based on a PIN or password exchange with the UE. Subsequent requests or responses after authorisation are only given priority by the P-CSCF and S-CSCF if some backwards indication is received for that specific dialog. The definition of this backwards indication is outside the scope of this document (because non-standardised mechanisms have already been implemented in association with this approach).
- 3) Authorisation based on subscription in the IM CN subsystem and on a database deployed by an AS; priority requested by the UE using a special dialstring. Specific dialstrings are configured in the P-CSCF. When a request is received from the UE by the P-CSCF, if the request contains a specific dialstring that is recognised by the P-CSCF as being eligible for priority treatment, the request is marked for temporary priority, subject to subsequent authorisation by an authorisation point (i.e., AS). Based on iFC functionality that exists at the S-CSCF (from the users subscription in the HSS), such requests are routed to an AS. Final authorisation is granted by the AS, based on a PIN or password exchange with the UE or based on user profile. Subsequent requests or responses after authorisation are only given priority by the P-CSCF and S-CSCF if some backwards indication is received for that specific dialog. The definition of this backwards indication is outside the scope of this document (because non-standardised mechanisms have already been implemented in association with this approach).

Some administrations can require the use of multiple approaches in the same network.

For the cases of interworking with other networks, where the P-CSCF of the other network does not support priority, but it is intended or required to give users of that P-CSCF priority in the home network, provision is made for recognition of dialstrings by the IBCF and the S-CSCF. In such scenarios, when the IBCF or S-CSCF recognize that a request contains a dialstring as being eligible for priority treatment, the request is marked by the IBCF or S-CSCF for temporary priority, subject to subsequent authorisation by an authorisation point (i.e. AS). This mechanism does not have an impact on the network where the P-CSCF resides.

Where the network has a requirement to prioritise emergency calls, it can either perform this function by the use of the "esnet" namespace in the Resource-Priority header field (as defined in RFC 7135 [197]), or by recognition of the presence of the service URN relating to an emergency. Where the Resource-Priority header field is used for this purpose, it is inserted by the entity identifying the emergency call, i.e. the P-CSCF or the IBCF. There is no usage of this namespace from the UE, and when this namespace is used, the trust domain implementation is set to remove it if it occurs from the UE.

## 4.12 Overload control

Usage of overload control is independent of the nature of any SIP using entity, i.e. there are no specific requirements for any particular IMS functional entity implementing SIP. The capability however is not extended to the UE except when performing the function of an externally attached network.

Two mechanisms are defined as follows:

- a feedback based mechanism defined in RFC 7339 [199], where the feedback is given in the Via header field of signalling messages supporting the traffic. RFC 7339 [199] also defines the default algorithm for usage of the feedback based mechanism in the IM CN subsystem (i.e. loss-based algorithm). Additional algorithms are either already defined, e.g. the rate-based scheme defined in RFC 7415 [200] or can also be defined in the future. As it is carried in the Via header fields the nature of the mechanism is hop by hop.
- an event package for distributing load filters defined in RFC 7200 [201], which can be either used in a hop-by-hop manner between adjacent entities in a similar manner to the feedback based mechanism, or can be used on a wider basis across the network, subject to the restrictions given in annex A. In this manner it can be used to address expected overload situations, e.g. for voting calls initiated by a specific television programme.

When the load filters based mechanism is used in the IMS, the default algorithm is loss-based (i.e. the filter specifies the relative percentage of incoming requests that can be accepted).

The S-CSCF, application servers and entities that implement the additional routing capability can use both mechanisms in parallel on the same interfaces.

There are no specific reasons why one protocol mechanism should be specified over another, although some discussion is given in the documents specifying the mechanisms themselves. It is regarded as a deployment issue as to which mechanisms are supported, and which algorithms are supported within those mechanisms, beyond those that the mechanisms themselves identify as mandatory. An operator will need to take a network wide view to planning their overload control strategy, it cannot be performed on ad-hoc basis as nodes are deployed. In particular, due regard has to be paid to emergency calls and priority calls in any overload control deployment, giving them priority in relation to other traffic consistent with what they are normally given.

For the distribution of load filters mechanism, typical deployments might include an S-CSCF subscribing to the load control event package at an AS, an AS subscribing to the load control event package at an AS, and an entity hosting additional routing capabilities as specified in subclause I.3 subscribing to the load-control event package at the AS.

Operation between two network operators is supported. If two network operators wish to implement overload control, it is a matter for bilateral agreement as to what is supported.

Operation with enterprise networks is supported. The network operator and the enterprise operator will need to agree on the overload control options to be supported.

---

## 5 Application usage of SIP

### 5.1 Procedures at the UE

#### 5.1.0 General

The UE procedures for UE detectable emergency calls are defined in subclause 5.1.6. Exceptions to UE procedures for SIP that do not relate to emergency, are documented in subclause 5.1.6 and shall apply. These exceptions include handling of a response to a request not detected by the UE as relating to an emergency.

#### 5.1.1 Registration and authentication

##### 5.1.1.1 General

The UE shall register public user identities (see table A.4/1 and dependencies on that major capability).

NOTE 1: The UE can use multiple Contact header field values simultaneously containing the same IP address and port number in the contact address.

In case a UE registers several public user identities at different points in time, the procedures to re-register, deregister and subscribe to the registration-state event package for these public user identities can remain uncoordinated in time.

The UE can register any one of its public user identities with any IP address acquired by the UE. The same public user identity can be bound to more than one IP address of the UE. While having valid registrations of previously registered public user identities, the UE can register any additional public user identity with any of its IP addresses. When binding any one of its public user identities to an additional contact address, the UE shall follow the procedures described in RFC 5626 [92].

If SIP digest without TLS is used, the UE shall not include signalling plane security mechanisms in the header fields defined in RFC 3329 [48] in any SIP messages.

NOTE 2: The UE determines if SIP digest is used with or without TLS based on device configuration. If SIP digest with TLS is used, then the UE includes the TLS signalling plane security mechanism in the header fields defined in RFC 3329 [48] as described in subclause 5.1.1.2.4.

SIP requests that indicate security mechanisms for both the signalling plane and the media plane can contain multiple instances or a single instance of the Security-Client, Security-Verify, or Security-Server header fields defined in RFC 3329 [48].

In case a device performing address and/or port number conversions is provided by a NA(P)T or NA(P)T-PT, the UE may need to modify the SIP contents according to the procedures described in either annex F or annex K.

NOTE 3: If UE populates the display-name of the Contact header field included in the REGISTER request with UE name, other UEs of the user can discover the UE name of the UE in the reg event package notification. The UE name is a text string chosen by the user allowing the user to distinguish individual UEs of the same user.

#### 5.1.1.1A Parameters contained in the ISIM

This subclause applies when a UE contains either an ISIM or a USIM.

The ISIM shall always be used for authentication to the IM CN subsystem, if it is present, as described in 3GPP TS 33.203 [19].

The ISIM is preconfigured with all the necessary parameters to initiate the registration to the IM CN subsystem. These parameters include:

- the private user identity;
- one or more public user identities; and
- the home network domain name used to address the SIP REGISTER request

The first public user identity in the list stored in the ISIM is used in emergency registration requests.

In case the UE does not contain an ISIM, the UE shall:

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to;

in accordance with the procedures in clause C.2.

The temporary public user identity is only used in REGISTER requests, i.e. initial registration, re-registration, UE-initiated deregistration.

The UE shall not reveal to the user the temporary public user identity if the temporary public user identity is barred. The temporary public user identity is not barred if received by the UE in the P-Associated-URI header field.

If the UE is unable to derive the parameters in this subclause for any reason, then the UE shall not proceed with the request associated with the use of these parameters and will not be able to register to the IM CN subsystem.



### 5.1.1.1B Parameters provisioned to a UE without ISIM or USIM

#### 5.1.1.1B.1 Parameters provisioned in the IMC

In case the UE contains neither an ISIM nor a USIM, but IMC is present the UE shall use preconfigured parameters in the IMC to initiate the registration to the IM CN subsystem and for authentication.

The following IMS parameters are assumed to be available to the UE:

- a private user identity;
- a public user identity; and
- a home network domain name to address the SIP REGISTER request to.

These parameters may not necessarily reside in a UICC.

The first public user identity in the list stored in the IMC is used in emergency registration requests.

#### 5.1.1.1B.2 Parameters when UE does not contain ISIM, USIM or IMC

If the UE contains neither ISIM, nor USIM nor IMC, the UE shall generate a temporary public user identity, a private user identity and a home network domain name to address the SIP REGISTER request to, according 3GPP TS 23.003 [3].

### 5.1.1.2 Initial registration

#### 5.1.1.2.1 General

The initial registration procedure consists of the UE sending an unprotected REGISTER request and, if challenged depending on the security mechanism supported for this UE, sending the integrity-protected REGISTER request or other appropriate response to the challenge. The UE can register a public user identity with any of its contact addresses at any time after it has acquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

When registering any public user identity belonging to the UE, the UE shall either use an already active pair of security associations or a TLS session to protect the REGISTER requests, or register the public user identity via a new initial registration procedure.

When binding any one of its public user identities to an additional contact address via a new initial registration procedure, the UE shall follow the procedures described in RFC 5626 [92]. The set of security associations or a TLS session resulting from this initial registration procedure will have no impact on the existing set of security associations or TLS sessions that have been established as a result of previous initial registration procedures. However, if the UE registers any one of its public user identities with a new contact address via a new initial registration procedure and does not employ the procedures described in RFC 5626 [92], then the new set of security associations or TLS session shall replace any existing set of security association or TLS session.

If the UE detects that the existing security associations or TLS sessions associated with a given contact address are no longer active (e.g., after receiving no response to several protected messages), the UE shall:

- consider all previously registered public user identities bound to this security associations or TLS session that are only associated with this contact address as deregistered; and
- stop processing all associated ongoing dialogs and transactions that were using the security associations or TLS session associated with this contact address, if any (i.e. no further SIP signalling will be sent by the UE on behalf of these transactions or dialogs).

The UE shall send the unprotected REGISTER requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, or if the UE was pre-configured with the P-CSCF's IP address or domain name and was unable to obtain specific port information, the UE shall send the unprotected REGISTER request to the SIP default port values as specified in RFC 3261 [26].

NOTE 1: The UE will only send further registration and subsequent SIP messages towards the same port of the P-CSCF for security mechanisms that do not require to use negotiated ports for exchanging protected messages.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B. A public user identity may be input by the end user.

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

- a) a From header field set to the SIP URI that contains:
  - 1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else
  - 2) the public user identity to be registered;
- b) a To header field set to the SIP URI that contains:
  - 1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else
  - 2) the public user identity to be registered;
- c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE:
  - 1) supports GRUU (see table A.4, item A.4/53);
  - 2) supports multiple registrations;
  - 3) has an IMEI available; or
  - 4) has an MEID available;

the UE shall include a "+sip.instance" header field parameter containing the instance ID. Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks.

NOTE 2: The requirement placed on the UE to include an instance ID based on the IMEI or the MEID when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62].

if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Contact URI without a user portion and containing the "bnc" URI parameter;

- d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDP is used. For TCP, the response is received on the TCP connection on which the request was sent. The UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in RFC 6223 [143];

NOTE 3: When sending the unprotected REGISTER request using UDP, the UE transmits the request from the same IP address and port on which it expects to receive the response to this request.

- e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 4: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

- f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;
- g) the Supported header field containing the option-tag "path", and
  - 1) if GRUU is supported, the option-tag "gruu"; and
  - 2) if multiple registrations is supported, the option-tag "outbound".
- h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4);
- i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7;

NOTE 5: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

- j) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Require header field containing the option-tag "gin"; and
- k) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Proxy-Require header field containing the option-tag "gin".

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

- a) if available, store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, the UE may initiate that mechanism on a media level when it initiates new media in an existing session.

NOTE 6: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

- a) store the expiration time of the registration for the public user identities found in the To header field value and bind it either to the respective contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used);

NOTE 7: If the UE supports RFC 6140 [191] and performs the functions of an external attached network, the To header field will contain the main URI of the UE.

- b) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header field and bind it to the respective contact address of the UE and the associated set of security associations or TLS session;

NOTE 8: When using the respective contact address and associated set of security associations or TLS session, the UE can utilize additional URIs contained in the P-Associated-URI header field and bound it to the respective contact address of the UE and the associated set of security associations or TLS session, e.g. for application purposes.

- c) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header field;
- d) store the list of service route values contained in the Service-Route header field and bind the list either to the contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session over which the REGISTER request was sent;

NOTE 9: When multiple registration mechanism is not used, there will be only one list of service route values bound to a contact address. However, when multiple registration mechanism is used, there will be different list of service route values bound to each registration flow and the associated contact address.

NOTE 10: The UE will use the stored list of service route values to build a proper preloaded Route header field for new dialogs and standalone transactions when using either the respective contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session.

e) if the UE indicated support for GRUU in the Supported header field of the REGISTER request then:

- if the UE did not use the procedures specified in RFC 6140 [191] for registration, find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered; and
- if the UE used the procedures specified in RFC 6140 [191] for registration then find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter then store the value of the "pub-gruu" header field parameter for use for generating public GRUUs for registering UAs as specified in RFC 6140 [191]. If this contains a "temp-gruu-cookie" header field parameter then store the value of the "temp-gruu-cookie" header field parameter for use for generating temporary GRUUs for registering UAs as specified in RFC 6140 [191];

NOTE 11: When allocating public GRUUs to registering UAs the functionality within the UE that performs the role of registrar will add an "sg" SIP URI parameter that uniquely identifies that UA to the public GRUU it received in the "pub-gruu" header field parameter. The procedures for generating a temporary GRUU using the "temp-gruu-cookie" header field parameter are specified in subclause 7.1.2.2 of RFC 6140 [191].

f) if the REGISTER request contained the "reg-id" and "+sip.instance" Contact header field parameter and the "outbound" option tag in a Supported header field, the UE shall check whether the option-tag "outbound" is present in the Require header field:

- if no option-tag "outbound" is present, the UE shall conclude that the S-CSCF does not support the registration procedure as described in RFC 5626 [92], and the S-CSCF has followed the registration procedure as described in RFC 5627 [93] or RFC 3261 [26], i.e., if there is a previously registered contact address, the S-CSCF replaced the old contact address and associated information with the new contact address and associated information (see bullet e) above). Upon detecting that the S-CSCF does not support the registration procedure as defined in RFC 5626 [92], the UE shall refrain from registering any additional IMS flows for the same private identity as described in RFC 5626 [92]; or

NOTE 12: Upon replacing the old contact address with the new contact address, the S-CSCF performs the network initiated deregistration procedure for the previously registered public user identities and the associated old contact address as described in subclause 5.4.1.5. Hence, the UE will receive a NOTIFY request informing the UE about the deregistration of the old contact address.

- if an option-tag "outbound" is present, the UE may establish additional IMS flows for the same private identity, as defined in RFC 5626 [92];

g) if available, store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, it may initiate that mechanism on a media level when it initiates new media in an existing session; and

NOTE 13: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

h) if the Via header field contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, start to send keep-alives associated with the registration towards the P-CSCF, as described in RFC 6223 [143].

On receiving a 305 (Use Proxy) response to the unprotected REGISTER request, unless otherwise specified in access specific annexes (as described in Annex B or Annex L), the UE shall:

- a) ignore the contents of the Contact header field if it is included in the received message;

NOTE 14: The 305 response is not expected to contain a Contact header field.

- b) release all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2;
- c) initiate either a new P-CSCF discovery procedure as described in subclause 9.2.1, or select a new P-CSCF, if the UE was pre-configured with more than one P-CSCF's IP addresses or domain names;
- d) select a P-CSCF address, which is different from the previously used address, from the address list; and
- e) perform the procedures for initial registration as described in subclause 5.1.1.2.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the registration expiration interval value with an expiration timer of at least the value received in the Min-Expires header field of the 423 (Interval Too Brief) response.

On receiving a 408 (Request Timeout) response or 500 (Server Internal Error) response or 504 (Server Time-Out) or 600 (Busy Everywhere) response for an initial registration, the UE may attempt to perform initial registration again.

When the timer F expires at the UE, the UE may:

- a) select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1 or from its pre-configured list of P-CSCF's IP addresses or domain names;
- b) if no response has been received when attempting to contact all P-CSCFs known by the UE, get a new set of P-CSCF-addresses as described in subclause 9.2.1 unless otherwise specified in the access specific annexes (as described in Annex B or Annex L); and
- c) perform the procedures for initial registration as described in subclause 5.1.1.2.

NOTE 15: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

On receiving a 4xx, 5xx or 6xx response to the REGISTER request, whereby the response contains a Retry-After header field, the UE shall not automatically attempt an initial registration via the same IP-CAN and the same P-CSCF for the amount of time indicated in the Retry-After header field. If the UE is power cycled, the UE can attempt an initial registration. If no initial registration occurs within the time period indicated by the Retry-After header field, the counter of unsuccessful initial registration attempts is reset.

After a first unsuccessful initial registration attempt, if the Retry-After header field was not present and the initial registration was not performed as a consequence of a failed reregistration, the UE shall not wait more than 5 minutes before attempting a new registration.

After a maximum of 2 consecutive unsuccessful initial registration attempts, if the Retry-After header field was not present in failure responses of those unsuccessful initial registration attempts, the UE shall implement the mechanism defined in subclause 4.5 of RFC 5626 [92] for new registration attempts. The UE shall use the values of the parameters max-time and base-time, of the algorithm defined in subclause 4.5 of RFC 5626 [92]. If no values of the parameters max-time and base-time have been provided to the UE by the network, the default values defined in subclause 4.5 of RFC 5626 [92] shall be used.

The values of max-time and base-time may be provided by the network to the UE using OMA-DM with the management objects specified in 3GPP TS 24.167 [8G]. Other mechanisms may be used as well and are outside the scope of the present specification.

#### 5.1.1.2.2 Initial registration using IMS AKA

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

- a) an Authorization header field, with:
  - the "username" header field parameter, set to the value of the private user identity;
  - the "realm" header field parameter, set to the domain name of the home network;

- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "nonce" header field parameter, set to an empty value; and
- the "response" header field parameter, set to an empty value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the port values see 3GPP TS 33.203 [19].

- b) additionally for the Contact header field, if the REGISTER request is protected by a security association, include the protected server port value in the hostport parameter;
- c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field; and
- d) a Security-Client header field set to specify the signalling plane security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the IPsec layer algorithms for integrity and confidentiality protection as defined in 3GPP TS 33.203 [19], and shall announce support for them according to the procedures defined in RFC 3329 [48].

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, the UE shall additionally:

- 1) If the UE supports multiple registrations and the REGISTER request contained the "+sip.instance" header field parameter and the "reg-id" header field parameter in the Contact header field, and the "outbound" option-tag in the Supported header field, the UE shall check whether the option-tag "outbound" is present in the Require header field. If the option-tag "outbound" is present, then the UE shall use the bidirectional flow as defined in RFC 5626 [92] as follows:
  - a) for UDP, the bidirectional flow consists of two unidirectional flows, i.e. the first unidirectional flow is identified with the UE's protected client port, the P-CSCF's protected server port, and the respective IP addresses. The UE uses this flow to send the requests and responses to the P-CSCF. The second unidirectional flow is identified with the P-CSCF's protected client port, the UE's protected server port and the IP addresses. The second unidirectional flow is used by the UE to receive the requests and responses from the P-CSCF; or
  - b) for TCP, the bidirectional flow is the TCP connection between the UE and the P-CSCF. This TCP connection was established by the UE, i.e. from the UE's protected client port and the UE's IP address to the P-CSCF's protected server port and the P-CSCF's IP address. This TCP connection is used to exchange SIP messages between the UE and the P-CSCF; and
- 2) set the security association lifetime to the longest of either the previously existing security association lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

NOTE 3: If the UE receives Authentication-Info, it will proceed as described in RFC 3310 [49].

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

### 5.1.1.2.3 Initial registration using SIP digest without TLS

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

- a) an Authorization header field as defined in RFC 2617 [21] unless otherwise specified in the access specific annexes, with:
  - the "username" header field parameter, set to the value of the private user identity;
  - the "realm" header field parameter, set to the domain name of the home network;

- the "uri" header field directive, set to the SIP URI of the domain name of the home network;
  - the "nonce" header field parameter, set to an empty value; and
  - the "response" header field parameter, set to an empty value;
- b) the hostport parameter in the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent requests; and
- c) the sent-by field in the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

The UE shall use the locally available public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration. The method whereby the public user identity and private user identity are made available to the UE is outside the scope of this document (e.g. a public user identity could be input by the end user).

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.4.

#### 5.1.1.2.4 Initial registration using SIP digest with TLS

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

- a) an Authorization header field set in accordance with subclause 5.1.1.2.3 unless otherwise specified in the access specific annexes; and
- b) a Security-Client header field set to specify the signalling plane security mechanism the UE supports. The UE shall support the setup of a TLS session as defined in 3GPP TS 33.203 [19]. The UE shall support the "tls" security mechanism, as specified in RFC 3329 [48]. The UE shall support TLS for integrity and confidentiality protection as defined in RFC 3261 [26], and shall announce support for them according to the procedures defined in RFC 3329 [48].

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, the UE shall additionally:

- a) set the TLS session lifetime to the longest of either the previously existing TLS session lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

If a UE supports TLS, then the UE shall support TLS ciphersuites as described in 3GPP TS 33.203 [19]. TLS session lifetime is determined by local configuration of the UE.

For SIP digest with TLS, the UE associates a protected server port with the TLS session port on the UE.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.6.

#### 5.1.1.2.5 Initial registration using NASS-IMS bundled authentication

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

- a) optionally, an Authorization header field, with the "username" header field parameter, set to the value of the private user identity;

NOTE 1: In case the Authorization header field is absent, the mechanism only supports that one public user identity is associated with only one private user identity. The public user identity is set so that it is possible to derive the private user identity from the public user identity by removing SIP URI scheme and the following parts of the SIP URI if present: port number, URI parameters, and To header field parameters.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, there are no additional requirements for the UE.

NOTE 2: When NASS-IMS bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

#### 5.1.1.2.6 Initial registration using GPRS-IMS-Bundled authentication

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

- a) an Authorization header field as defined in RFC 2617 [21] shall not be included, in order to indicate support for GPRS-IMS-Bundled authentication.
- b) the Security-Client header field as defined in RFC 3329 [48] shall not contain signalling plane security mechanisms;
- c) a From header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003 [3], as the public user identity to be registered;
- d) a To header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003 [3], as the public user identity to be registered;
- e) the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests; and
- f) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

NOTE 1: Since the private user identity is not included in the REGISTER requests when GPRS-IMS-Bundled authentication is used for registration, re-registration and de-registration procedures, all REGISTER requests from the UE use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. The UE does not use the temporary public user identity (IMSI-derived IMPU) in any non-registration SIP requests.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, there are no additional requirements for the UE.

NOTE 2: When GPRS-IMS-Bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

#### 5.1.1.3 Subscription to the registration-state event package

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680 [43].

NOTE 1: If the UE supports RFC 6140 [191] and performs the functions of an external attached network, the subscription will be directed to the main URI, as described in RFC 6140 [191].

The UE shall subscribe to the reg event package upon registering a new contact address via an initial registration procedure. If the UE receives a NOTIFY request via the newly established subscription dialog and via the previously established subscription dialogs (there will be at least one), the UE may terminate the previously established subscription dialogs and keep only the newly established subscription dialog.

The UE shall use the default public user identity for subscription to the registration-state event package.

NOTE 2: The subscription information stored in the HSS ensures that the default public user identity is a SIP URI.

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

- a) a Request-URI set to the resource to which the UE wants to be subscribed to, i.e. to the SIP URI that is the default public user identity used for subscription;
- b) a From header field set to the SIP URI that is the default public user identity used for subscription;
- c) a To header field set to the SIP URI that is the default public user identity used for subscription;
- d) an Event header field set to the "reg" event package;
- e) an Expires header field set to 600 000 seconds as the value desired for the duration of the subscription;
- f) void; and



g) void.

Upon receipt of a 2xx response to the SUBSCRIBE request, the UE shall store the information for the established dialog and the expiration time as indicated in the Expires header field of the received response.

If continued subscription is required, the UE shall automatically refresh the subscription by the reg event package, for a previously registered public user identity, either 600 seconds before the expiration time if the initial subscription was for greater than 1200 seconds, or when half of the time has expired if the initial subscription was for 1200 seconds or less. If a SUBSCRIBE request to refresh a subscription fails with a non-481 response, the UE shall still consider the original subscription valid for the duration of the most recently known "Expires" value according to RFC 3265 [28]. Otherwise, the UE shall consider the subscription invalid and start a new initial subscription according to RFC 3265 [28].

#### 5.1.1.3A Void

### 5.1.1.4 User-initiated reregistration and registration of an additional public user identity

#### 5.1.1.4.1 General

The UE can perform the reregistration of a previously registered public user identity bound to any one of its contact addresses and the associated set of security associations or TLS sessions at any time after the initial registration has been completed.

The UE can perform the reregistration of a previously registered public user identity over any existing set of security associations or TLS session that is associated with the related contact address.

The UE can perform the reregistration of a previously registered public user identity via an initial registration as specified in subclause 5.1.1.2, when binding the previously registered public user identity to new contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used).

The UE can perform registration of additional public user identities at any time after the initial registration has been completed. The UE shall perform the registration of additional public user identities either:

- over the existing set of security associations or TLS sessions, if appropriate to the security mechanism in use, that is associated with the related contact address; or
- via an initial registration as specified in subclause 5.1.1.2.

The UE can fetch bindings as defined in RFC 3261 [26] at any time after the initial registration has been completed. The procedure for fetching bindings is the same as for a reregistration except that the REGISTER request does not contain a Contact header field.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister an already registered public user identity either 600 seconds before the expiration time if the previous registration was for greater than 1200 seconds, or when half of the time has expired if the previous registration was for 1200 seconds or less, or when the UE intends to update its capabilities according to RFC 3840 [62] or when the UE needs to modify the ICSI values that the UE intends to use in a g.3gpp.icsi-ref media feature tag or IARI values that the UE intends to use in the g.3gpp.iari-ref media feature tag.

When sending a protected REGISTER request, the UE shall use a security association or TLS session associated either with the contact address or to the registration flow and the associated contact address used to send the request, see 3GPP TS 33.203 [19], established as a result of an earlier initial registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

- a) a From header field set to the SIP URI that contains:
  - 1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

- 2) the public user identity to be registered;
- b) a To header field set to the SIP URI that contains:
  - 1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else
  - 2) the public user identity to be registered;
- c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE:
  - 1) supports GRUU (see table A.4, item A.4/53);
  - 2) supports multiple registrations;
  - 3) has an IMEI available; or
  - 4) has an MEID available.

Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks.

NOTE 1: The requirement placed on the UE to include an instance ID based on the IMEI or the MEID when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62].

if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Contact URI without a user portion and containing the "bnc" URI parameter;

- d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continuous support to send keep-alives, as described in RFC 6223 [143];
- e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 2: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

- f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;
- g) the Supported header field containing the option-tag "path", and:
  - 1) if GRUU is supported, the option-tag "gruu"; and
  - 2) if multiple registrations is supported, the option-tag "outbound";
- h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4);
- i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7;

NOTE 3: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

- j) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Require header field containing the option-tag "gin"; and
- k) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Proxy-Require header field containing the option-tag "gin".

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

- a) bind the new expiration time of the registration for this public user identity found in the To header field value either to the contact address or to the registration flow and the associated contact address used in this registration;

NOTE 4: If the UE supports RFC 6140 [191] and performs the functions of an external attached network, the To header field will contain the main URI of the UE.

- b) store the list of service route values contained in the Service-Route header field and bind the list either to the contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used);

NOTE 5: The stored list of service route values will be used to build a proper preloaded Route header field for new dialogs and standalone transactions when using either the respective contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used).

NOTE 6: If the list of Service-Route headers saved from a previous registration and bound either to this contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session already exist, then the received list of Service-Route headers replaces the old list.

NOTE 7: The UE can utilize additional URIs contained in the P-Associated-URI header field, e.g. for application purposes.

- c) if the UE indicated support for GRUU in the Supported header field of the REGISTER request then:
  - if the UE did not use the procedures specified in RFC 6140 [191] for registration find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered; and
  - if the UE used the procedures specified in RFC 6140 [191] for registration then find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter then store the value of the "pub-gruu" header field parameter for use for generating public GRUUs for registering UAs as specified in RFC 6140 [191]. If this contains a "temp-gruu-cookie" header field parameter then store the value of the "temp-gruu-cookie" header field parameter for use for generating temporary GRUUs for registering UAs as specified in RFC 6140 [191];

NOTE 8: When allocating public GRUUs to registering UAs the functionality within the UE that performs the role of registrar will add an "sg" SIP URI parameter that uniquely identifies that UA to the public GRUU it received in the "pub-gruu" header field parameter. The procedures for generating a temporary GRUU using the "temp-gruu-cookie" header field parameter are specified in subclause 7.1.2.2 of RFC 6140 [191].

- d) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field and labelled with the "mediasec" header field parameter specified in subclause 7.2A.7, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, it may initiate that mechanism on a media level when it initiates new media in an existing session; and

NOTE 9: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

- e) if the Via header field contains a "keep" header field parameter with a value, continue to send keep-alives as described in RFC 6223 [143], towards the P-CSCF.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the registration expiration interval value with an expiration timer of at least the value received in the Min-Expires header field of the 423 (Interval Too Brief) response.

On receiving a 408 (Request Timeout) response or 500 (Server Internal Error) response or 504 (Server Time-Out) response for a reregistration, the UE shall perform the procedures for initial registration as described in subclause 5.1.1.2.

On receiving a 305 (Use Proxy) response to the REGISTER request, unless otherwise specified in the access specific annexes (as described in Annex B or Annex L), the UE shall:

- a) ignore the contents of the Contact header field if it is included in the received message;

NOTE 4: The 305 response is not expected to contain a Contact header field.

- b) release all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2;
- c) initiate either a new P-CSCF discovery procedure as described in subclause 9.2.1, or select a new P-CSCF, if the UE was pre-configured with more than one P-CSCF's IP addresses or domain names;
- d) select a P-CSCF address, which is different from the previously used address, from the address list; and
- e) perform the procedures for initial registration as described in subclause 5.1.1.2.

When the timer F expires at the UE:

- 1) the UE shall stop processing of all ongoing dialogs and transactions associated with that flow, if any (i.e. no further SIP signalling will be sent by the UE on behalf of these transactions or dialogs); and
- 2) after releasing all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2:
  - a) the UE may select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1 or from its pre-configured list of P-CSCF's IP addresses or domain names;
  - b) if no response has been received when attempting to contact all P-CSCFs known by the UE, the UE may get a new set of P-CSCF-addresses as described in subclause 9.2.1 unless otherwise specified in the access specific annexes (as described in Annex B or Annex L);
  - c) the UE may perform the procedures for initial registration as described in subclause 5.1.1.2; and
  - d) the UE shall perform the procedures in RFC 5626 [92] to form a new flow to replace the failed one if it supports multiple registrations. If failed registration attempts occur in the process of creating a new flow, the flow recovery procedures defined in RFC 5626 [92] shall apply. The UE shall use the values of the parameters max-time and base-time, of the algorithm defined in subclause 4.5 of RFC 5626 [92]. If no values of the parameters max-time and base-time have been provided to the UE by the network, the default values defined in in subclause 4.5 of RFC 5626 [92] shall be used.

NOTE 10: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

#### 5.1.1.4.2 IMS AKA as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

- a) an Authorization header field, with:
  - the "username" header field parameter set to the value of the private user identity;
  - the "realm" header field parameter directive, set to the value as received in the "realm" WWW-Authenticate header field parameter;

- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "nonce" header field parameter, set to last received nonce value; and
- the "response" header field parameter, set to the last calculated response value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

NOTE 3: If the UE is setting up an additional registration using procedures specified in RFC 5626 [92] and the UE accesses the network through 3GPP or 3GPP2 systems without any NAT, the flow is considered to be "logical flow".

- b) additionally for the Contact header field, include the protected server port value in the hostport parameter;
- c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field;
- d) a Security-Client header field, set to specify the signalling plane security mechanism it supports, the IPsec layer algorithms for security and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]; and
- e) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

On receiving the 200 (OK) response to the REGISTER request, the UE shall additionally:

- a) set the security association lifetime associated with either this contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

NOTE 4: If the UE receives Authentication-Info, it will proceed as described in RFC 3310 [49].

#### 5.1.1.4.3 SIP digest without TLS as a security mechanism

On sending a REGISTER request that does not contain a challenge response, the UE shall additionally populate the header fields as follows:

- a) an Authorization header field as defined in RFC 2617 [21], including:
  - the "username" header field parameter, set to the value of the private user identity;
  - the "realm" header field parameter, set to the domain name of the home network;
  - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
  - the "nonce" header field parameter, set to an empty value; and
  - the "response" header field parameter, set to an empty value;
- b) the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent requests; and
- c) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

#### 5.1.1.4.4 SIP digest with TLS as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

- a) an Authorization header field set in accordance with subclause 5.1.1.2.3;
- b) the Security-Client header field set to specify the signalling plane security mechanism the UE supports. The UE shall support the setup of a TLS session as defined in 3GPP TS 33.203 [19]. The UE shall support the "tls" security mechanism, as specified in RFC 3329 [48]. The UE shall support TLS for integrity and confidentiality protection as defined in RFC 3261 [26], and shall announce support for them according to the procedures defined in RFC 3329 [48]; and
- c) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, the UE shall additionally:

- a) set the lifetime of the respective TLS session to the value configured.

#### 5.1.1.4.5 NASS-IMS bundled authentication as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

- a) optionally, an Authorization header field, with the "username" header field parameter, set to the value of the private user identity;

NOTE 1: In case the Authorization header field is absent, the mechanism only supports that one public user identity is associated with only one private user identity.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, there are no additional requirements for the UE.

NOTE 2: When NASS-IMS bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

#### 5.1.1.4.6 GPRS-IMS-Bundled authentication as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

- a) an Authorization header field as defined in RFC 2617 [21] shall not be included, in order to indicate support GPRS-IMS-Bundled authentication.
- b) security agreement header field values as required by RFC 3329 [48] shall not contain signalling plane security mechanisms;
- c) a From header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003 [3], as the public user identity to be registered;
- d) a To header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003 [3], as the public user identity to be registered;
- e) the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests; and
- f) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

NOTE 1: Since the private user identity is not included in the REGISTER requests when GPRS-IMS-Bundled authentication is used for registration, re-registration and de-registration procedures, all REGISTER requests from the UE use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. The UE does not use the temporary public user identity (IMSI-derived IMPU) in any non-registration SIP requests.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.4.1, there are no additional requirements for the UE.

NOTE 2: When GPRS-IMS-Bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

## 5.1.1.5 Authentication

### 5.1.1.5.1 IMS AKA - general

Authentication is performed during initial registration. A UE can be re-authenticated during subsequent reregistrations, deregistrations or registrations of additional public user identities. When the network requires authentication or re-authentication of the UE, the UE will receive a 401 (Unauthorized) response to the REGISTER request.

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

- 1) extract the RAND and AUTN parameters;
- 2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and
- 3) check the existence of the Security-Server header field as described in RFC 3329 [48]. If the Security-Server header field is not present or it does not contain the parameters required for the setup of the set of security associations (see annex H of 3GPP TS 33.203 [19]), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

- 1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203 [19];
- 2) set up a temporary set of security associations for this registration based on the static list and parameters the UE received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header field in the REGISTER request. The UE sets up the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK and CK (only if encryption enabled) as the shared key. The UE shall use the parameters received in the Security-Server header field to setup the temporary set of security associations. The UE shall set a temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer;
- 3) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field and labelled with the "mediasec" header field parameter specified in subclause 7.2A.7, if any

NOTE 1: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

- 4) send another REGISTER request towards the protected server port indicated in the response using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial REGISTER request that was challenged with the received 401 (Unauthorized) response, with the addition that the UE shall include an Authorization header field containing:
  - the "realm" header field parameter set to the value as received in the "realm" WWW-Authenticate header field parameter;
  - the "username" header field parameter, set to the value of the private user identity;
  - the "response" header field parameter that contains the RES parameter, as described in RFC 3310 [49];
  - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
  - the "algorithm" header field parameter, set to the value received in the 401 (Unauthorized) response; and
  - the "nonce" header field parameter, set to the value received in the 401 (Unauthorized) response.

The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the security association protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

NOTE 2: The Security-Client header field contains signaling plane security mechanism and if the UE supports media plane security, then media plane security mechanisms are contained, too.

On receiving the 200 (OK) response for the security association protected REGISTER request registering a public user identity with the associated contact address, the UE shall:

- change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and
- if this is the only set of security associations available toward the P-CSCF, use the newly established set of security associations for further messages sent towards the P-CSCF. If there are additional sets of security associations (e.g. due to registration of multiple contact addresses), the UE can either use them or use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

NOTE 3: If the UE has registered multiple contact addresses, the UE can either send requests towards the P-CSCF over the newly established set of security associations, or use different UE's contact address and associated set of security associations when sending the requests towards the P-CSCF. Responses towards the P-CSCF that are sent via UDP will be sent over the same set of security associations that the related request was received on. Responses towards the P-CSCF that are sent via TCP will be sent over the same set of security associations that the related request was received on.

When the first request or response protected with the newly established set of security associations is received from the P-CSCF or when the lifetime of the old set of security associations expires, the UE shall delete the old set of security associations and related keys it may have with the P-CSCF after all SIP transactions that use the old set of security associations are completed.

NOTE 4: If the UE has registered multiple contact addresses, the S-CSCF can use different contact address when sending the requests destined for the UE. In this case the UE will not receive the subsequent requests over the newly established set of security associations.

Whenever the 200 (OK) response is not received before the temporary SIP level lifetime of the temporary set of security associations expires or a 403 (Forbidden) response is received, the UE shall consider the registration to have failed. The UE shall delete the temporary set of security associations it was trying to establish, and use the old set of security associations. The UE should send an unprotected REGISTER request according to the procedure specified in subclause 5.1.1.2 if the UE considers the old set of security associations to be no longer active at the P-CSCF.

In the case that the 401 (Unauthorized) response is deemed to be invalid then the UE shall behave as defined in subclause 5.1.1.5.3.

#### 5.1.1.5.2 Void

#### 5.1.1.5.3 IMS AKA abnormal cases

If, in a 401 (Unauthorized) response, either the MAC or SQN is incorrect the UE shall respond with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid as follows:

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no "auts" Authorization header field parameter and an empty "response" Authorization header field parameter, i.e. no authentication challenge response;
- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the "auts" Authorization header field parameter (see 3GPP TS 33.102 [18]).

NOTE: In the case of the SQN being out of range, a "response" Authorization header field parameter can be included by the UE, based on the procedures described in RFC 3310 [49].

Whenever the UE detects any of the above cases, the UE shall:

- send the REGISTER request using an existing set of security associations, if available (see 3GPP TS 33.203 [19]);
- populate a new Security-Client header field within the REGISTER request and associated contact address, set to specify the security mechanisms it supports, the IPsec layer algorithms for integrity and confidentiality protection it supports and the parameters needed for the new security association setup; and



- not create a temporary set of security associations.

On receiving a 420 (Bad Extension) in which the Unsupported header field contains the value "sec-agree" and if the UE supports GPRS-IMS-Bundled authentication, the UE shall initiate a new authentication attempt with the GPRS-IMS-Bundled authentication procedures as specified in subclause 5.1.1.2.6.

#### 5.1.1.5.4 SIP digest without TLS – general

On receiving a 401 (Unauthorized) response to the REGISTER request, and where the "algorithm" Authorization header field parameter is "MD5", the UE shall extract the digest-challenge parameters as indicated in RFC 2617 [21] from the WWW-Authenticate header field. The UE shall calculate digest-response parameters as indicated in RFC 2617 [21]. The UE shall send another REGISTER request containing an Authorization header field. The header fields are populated as defined in subclause 5.1.1.2.3, with the addition that the UE shall include an Authorization header field containing a challenge response, i.e. "nonce", "qop", and "nonce-count" header field parameters as indicated in RFC 2617 [21]. The UE shall set the Call-ID of the REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge. If SIP digest without TLS is used, the UE shall not include RFC 3329 [48] header fields with this REGISTER.

On receiving the 200 (OK) response for the REGISTER request, if the "algorithm" Authentication-Info header field parameter is "MD5", the UE shall authenticate the S-CSCF using the "rspauth" Authentication-Info header field parameter as described in RFC 2617 [21]. If the nextnonce field is present in the Authentication-Info header field the UE should use it when constructing the Authorization header for its next request as specified in RFC 2617 [21].

#### 5.1.1.5.5 SIP digest without TLS – abnormal procedures

On receiving a 403 (Forbidden) response, the UE shall consider the registration to have failed.

#### 5.1.1.5.6 SIP digest with TLS – general

On receiving a 401 (Unauthorized) response to the REGISTER request, the procedures in subclause 5.1.1.5.4 apply with the following differences:

- The UE shall check the existence of the Security-Server header field as described in RFC 3329 [48]. If the Security-Server header field is not present or the list of supported security mechanisms does not include "tls", the UE shall abandon the authentication procedure and send a new REGISTER request.

In the case that the 401 (Unauthorized) response to the REGISTER is deemed to be valid the UE shall:

- store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any; and

NOTE 1: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

- send another REGISTER request using the TLS session to protect the message.

The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header field containing a challenge response, "nonce", "qop", and "nonce-count" header field parameters as indicated in RFC 2617 [21]. The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

NOTE 2: The Security-Client header field contains signaling plane security mechanism and if the UE supports media plane security, then media plane security mechanisms are contained, too.

When SIP digest with TLS is used, and for the case where the 401 (Unauthorized) response to the REGISTER request is deemed to be valid, the UE shall establish the TLS session as described in 3GPP TS 33.203 [19]. The UE shall use this TLS session to send all further messages towards the P-CSCF towards the protected server port.

#### 5.1.1.5.7 SIP digest with TLS – abnormal procedures

On receiving a 403 (Forbidden) response, the UE shall consider the registration to have failed. If performing SIP digest with TLS, the UE should send an initial REGISTER according to the procedure specified in subclause 5.1.1.2 if the UE considers the TLS session to be no longer active at the P-CSCF.

#### 5.1.1.5.8 NASS-IMS bundled authentication – general

NASS-IMS bundled authentication is only applicable to UEs that contain neither USIM nor ISIM. Authentication is achieved via the registration and re-registration procedures as defined in subclause 5.1.1.2 and subclause 5.1.1.4. NASS-bundled authentication is granted by the network upon receipt by the UE of a 200 (OK) response to the initial REGISTER request.

There is no separate authentication procedure.

#### 5.1.1.5.9 NASS-IMS bundled authentication – abnormal procedures

There is no separate authentication procedure, and therefore no abnormal procedures.

#### 5.1.1.5.10 GPRS-IMS-Bundled authentication – general

Authentication is achieved via the registration and re-registration procedures as defined in subclause 5.1.1.2 and subclause 5.1.1.4. GPRS-IMS-Bundled authentication is granted by the network upon receipt by the UE of a 200 (OK) response to the initial REGISTER request.

#### 5.1.1.5.11 GPRS-IMS-Bundled authentication – abnormal procedures

There is no separate authentication procedure and therefore no abnormal procedures.

#### 5.1.1.5.12 Abnormal procedures for all security mechanisms

A UE shall only respond to two consecutive invalid challenges and shall not automatically attempt authentication after two consecutive failed attempts to authenticate. The UE may attempt to register with the network again after an implementation specific time.

#### 5.1.1.5A Network-initiated re-authentication

At any time, the UE can receive a NOTIFY request carrying information related to the reg event package (as described in subclause 5.1.1.3). If:

- the state attribute in any of the <registration> elements is set to "active";
- the value of the <uri> sub-element inside the <contact> sub-element is set to the Contact address that the UE registered; and
- the event attribute of that <contact> sub-element(s) is set to "shortened";

the UE shall:

- 1) use the expiry attribute within the <contact> sub-element that the UE registered to adjust the expiration time for that public user identity; and
- 2) start the re-authentication procedures at the appropriate time (as a result of the S-CSCF procedure described in subclause 5.4.1.6) by initiating a reregistration as described in subclause 5.1.1.4, if required.

**NOTE:** When authenticating a given private user identity, the S-CSCF will only shorten the expiry time within the <contact> sub-element that the UE registered using its private user identity. The <contact> elements for the same public user identity, if registered by another UE using different private user identities remain unchanged. The UE will not initiate a reregistration procedure, if none of its <contact> sub-elements was modified.

#### 5.1.1.5B Change of IPv6 address due to privacy

Stateless address autoconfiguration as described in RFC 2462 [20E] defines how an IPv6 prefix and an interface identifier is used by the UE to construct a complete IPv6 address.

If the UE receives an IPv6 prefix, the UE may change the interface identity of the IPv6 address as described in RFC 3041 [25A] due to privacy but this can result in service discontinuity for services provided by the IM CN subsystem.

**NOTE:** When the UE constructs new IPv6 address by changing the interface identity, the UE can either transfer all established dialogs to new IPv6 address as specified in 3GPP TS 24.237 [8M] and subsequently relinquish the old IPv6 address, or terminate all established dialogs and transactions. While transferring the established dialogs to new IPv6 address, the UE will have double registration, i.e. one registration for the old IPv6 address and another for the new IPv6 address.

The procedure described below assumes that the UE will terminate all established dialogs and transactions and temporarily disconnect the UE from the IM CN subsystem until the new registration is performed. If the UE decides to change the IPv6 address due to privacy and terminate all established dialogs and transaction, associated with old IPv6 address, the UE shall:

- 1) terminate all ongoing dialogs (e.g., sessions) and transactions (e.g., subscription to the reg event) that were using the old IPv6 address;
- 2) deregister all registered public user identities that were using the old IPv6 address as described in subclause 5.1.1.4;
- 3) construct a new IPv6 address according to the procedures specified in RFC 3041 [25A];
- 4) register the public user identities that were deregistered in step 2 above with a new IPv6 address, as follows:
  - a) by performing an initial registration as described in subclause 5.1.1.2; and
  - b) by performing a subscription to the reg event package as described in subclause 5.1.1.3; and
- 5) subscribe to other event packages it was subscribed to before the change of IPv6 address procedure started.

To ensure a maximum degree of continuous service to the end user, the UE should transfer all established dialogs to the new IPv6 address as specified in 3GPP TS 24.237 [8M] rather than terminate all established dialogs and transactions and temporarily disconnect the UE from the IM CN subsystem as described above.

## 5.1.1.6 User-initiated deregistration

### 5.1.1.6.1 General

For any public user identity that the UE has previously registered, the UE can deregister via a single registration procedure:

- all contact addresses bound to the indicated public user identity;
- some contact addresses bound to the indicated public user identity;
- a particular contact address bound to the indicated public user identity; or
- when the UE supports multiple registrations (i.e. the "outbound" option tag is included in the Supported header field) one or more flows bound to the indicated public user identity.

The UE can deregister a public user identity that it has previously registered with its contact address at any time. The UE shall protect the REGISTER request using a security association or TLS session that is associated with contact address, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if one is available.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

Prior to sending a REGISTER request for deregistration, the UE shall release all dialogs that were using the contact addresses or the flow that is going to be deregistered and related to the public user identity that is going to be deregistered or to one of the implicitly registered public user identities. However:

- if the dialog that was established by the UE subscribing to the reg event package used the public user identity that is going to be deregistered; and

- this dialog is the only remaining dialog used for subscription to reg event package of the user, i.e. there are no other contact addresses registered with associated subscription to the reg event package of the user;

then the UE shall not release this dialog.

On sending a REGISTER request that will remove the binding between the public user identity and one of its contact addresses or one of its flows, the UE shall populate the header fields as follows:

- a) a From header field set to the SIP URI that contains:
  - 1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else
  - 2) the public user identity to be deregistered;
- b) a To header field set to the SIP URI that contains:
  - 1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else
  - 2) the public user identity to be deregistered;
- c) a Contact header field set to the SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN, and:
  - 1) if the UE is removing the binding between the public user identity indicated in the To header field, (together with the associated implicitly registered public user identities), and the contact address indicated in the Contact header field; and
    - if the UE supports GRUU, or multiple registrations (i.e. the "outbound" option tag is included in the Supported header field), or has an IMEI available, or has an MEID available, the Contact header field also contains the "+sip.instance" header field parameter. Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks;
    - if the UE supports multiple registrations (i.e. the "outbound" option tag is included in the Supported header field), the Contact header field does not contain the "reg-id" header field parameter;
    - if the UE does not support GRUU and does not support multiple registrations (i.e. the "outbound" option tag is not included in the Supported header field), and does not have an IMEI available, and does not have an MEID available, the Contact header field does not contain either the "+sip.instance" header field parameter or the "reg-id" header field parameter;

NOTE 1: Since the contact address is deregistered, if there are any flows that were previously registered with the respective contact address, all flows terminating at the respective contact address are removed.

- 2) if the UE is removing the binding between the public user identity indicated in the To header field, (together with the associated implicitly registered public user identities) and one of its flows, the Contact header field contains the "+sip.instance" header field parameter and the "reg-id" header field parameter that identifies the flow; and

NOTE 2: The requirement placed on the UE to include an instance ID based on the IMEI when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

- 3) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Contact URI without a user portion and containing the "bnc" URI parameter;
- d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field;
  - e) a registration expiration interval value set to the value of zero, appropriate to the deregistration requirements of the user;
  - f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

- g) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4);
- h) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any;

NOTE 3: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

- i) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Require header field containing the option-tag "gin"; and
- j) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Proxy-Require header field containing the option-tag "gin".

For a public user identity that the UE has registered with multiple contact addresses or multiple flows (e.g. via different P-CSCFs), the UE shall also be able to deregister multiple contact addresses or multiple flows, bound to its public user identity, via single deregistration procedure as specified in RFC 3261 [26]. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a list of Contact headers. Each Contact header field is populated as specified above in bullets a) through i).

The UE can deregister all contact addresses bound to its public user identity and associated with its private user identity. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a public user identity that is being deregistered in the To header field, and a single Contact header field with value of "\*" and the Expires header field with a value of "0". The UE shall not include the "instance-id" feature tag and the "reg-id" header field parameter in the Contact header field in the REGISTER request.

NOTE 4: All entities subscribed to the reg event package of the user will be inform via NOTIFY request which contact addresses bound to the public user identity have been deregistered.

When a 401 (Unauthorized) response to a REGISTER request is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

- remove all registration details relating to this public user identity and the associated contact address.
- store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any.

NOTE 5: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

If there are no more public user identities registered with this contact address, the UE shall delete any stored media plane security mechanisms and related keys and any security associations or TLS sessions and related keys it may have towards the IM CN subsystem.

If all public user identities are deregistered and all security association or TLS session is removed, then the UE shall consider subscription to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header field containing a value of zero).

#### 5.1.1.6.2 IMS AKA as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.6.1, the UE shall additionally populate the header fields as follows:

- a) an Authorization header field, with:
  - the "username" header field parameter, set to the value of the private user identity;
  - the "realm" header field parameter, set to the value as received in the "realm" WWW-Authenticate header field parameter;
  - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

- the "nonce" header field parameter, set to last received nonce value; and
  - the response directive, set to the last calculated response value;
- b) additionally for each Contact header field and associated contact address, include the associated protected server port value in the hostport parameter;
- c) additionally for the Via header field, include the protected server port value bound to the security association in the sent-by field;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

- d) a Security-Client header field, set to specify the signalling plane security mechanisms it supports, the IPsec layer algorithms for integrity and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]; and
- e) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

NOTE 2: When the UE has received the 200 (OK) response for the REGISTER request of the only public user identity currently registered with this contact address and its associated set of implicitly registered public user identities (i.e. no other public user identity is registered), the UE removes the security association (between the P-CSCF and the UE) that were using this contact address. Therefore further SIP signalling using this security association (e.g. the NOTIFY request containing the deregistration event) will not reach the UE.

#### 5.1.1.6.3 SIP digest without TLS as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.6.1, the UE shall additionally populate the header fields as follows:

- a) an Authorization header field as defined in RFC 2617 [21], including:
- the "username" header field parameter, set to the value of the private user identity;
  - the "realm" header field parameter, set to the domain name of the home network;
  - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
  - the "nonce" header field parameter, set to an empty value; and
  - the "response" header field parameter, set to an empty value;
- b) for each Contact header field and associated contact address include the associated unprotected port value (where the UE was expecting to receive mid-dialog requests); and
- c) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

#### 5.1.1.6.4 SIP digest with TLS as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.6.1, the UE shall additionally populate the header fields as follows:

- a) an Authorization header field set in accordance with subclause 5.1.1.6.3; and
- b) a Security-Client header field, set to specify the signalling plane security mechanism it supports. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]; and
- c) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

#### 5.1.1.6.5 NASS-IMS bundled authentication as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.6.1, the UE shall additionally populate the header fields as follows:

- a) optionally, an Authorization header field, with the "username" header field parameter, set to the value of the private user identity;

NOTE 1: In case the Authorization header field is absent, the mechanism only supports that one public user identity is associated with only one private user identity.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.6.1, there are no additional requirements for the UE.

NOTE 2: When NASS-IMS bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

#### 5.1.1.6.6 GPRS-IMS-Bundled authentication as a security mechanism

On sending a REGISTER request, as defined in subclause 5.1.1.6.1, the UE shall additionally populate the header fields as follows:

- a) an Authorization header field as defined in RFC 2617 [21] shall not be included, in order to indicate support GPRS-IMS-Bundled authentication.
- b) the Security-Verify header field and the Security-Client header field values as defined by RFC 3329 [48] shall not contain signalling plane security mechanisms;
- c) a From header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003 [3], as the public user identity to be deregistered;
- d) a To header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003 [3], as the public user identity to be deregistered;
- e) for each Contact header field and associated contact address include the associated unprotected port value (where the UE was expecting to receive mid-dialog requests); and
- f) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

NOTE 1: Since the private user identity is not included in the REGISTER requests when GPRS-IMS-Bundled authentication is used for registration, re-registration and de-registration procedures, all REGISTER requests from the UE use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. The UE does not use the temporary public user identity (IMSI-derived IMPU) in any non-registration SIP requests.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.6.1, there are no additional requirements for the UE.

NOTE 2: When GPRS-IMS-Bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

#### 5.1.1.7 Network-initiated deregistration

Upon receipt of a NOTIFY request, on any dialog which was generated during the subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) which were registered by this UE, with:

- 1) the state attribute within the <registration> element set to "terminated", and within each <contact> element belonging to this UE, the state attribute set to "terminated" and the event attribute set either to "unregistered", or "rejected", or "deactivated", the UE shall remove all registration details relating to the respective public user identity (i.e. consider the public user identity indicated in the aor attribute of the <registration> element as deregistered); or
- 2) the state attribute within the <registration> element set to "active", and within a given <contact> element belonging to this UE, the state attribute set to "terminated", and the associated event attribute set either to

"unregistered", or "rejected" or "deactivated", the UE shall consider the binding between the public user identity and either the contact address or the registration flow and the associated contact address (if the multiple registration mechanism is used) indicated in the respective <contact> element as removed. The UE shall consider its public user identity as deregistered when all bindings between the respective public user identity and all contact addresses and all registration flow and the associated contact address (if the multiple registration mechanism is used) belonging to this UE are removed.

NOTE 1: When multiple registration mechanism is used to register a public user identity and bind it to a registration flow and the associated contact address, there will be one <contact> element for each registration flow and the associated contact address.

NOTE 2: If the state attribute within the <registration> element is set to "active" and the <contact> element belonging to this UE is set to "active", the UE will consider that the binding between the public user identity and either the respective contact address or the registration flow and the associated contact address as left unchanged.

In case of a "deactivated" event attribute, the UE shall start the initial registration procedure as described in subclause 5.1.1.2. In case of a "rejected" event attribute, the UE shall release all dialogs related to those public user identities.

Upon receipt of a NOTIFY request, the UE shall delete all security associations or TLS sessions towards the P-CSCF either:

- if all <registration> element(s) have their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header field contains the value of "terminated"; or
- if each <registration> element that was registered by this UE has either the state attribute set to "terminated", or the state attribute set to "active" and the state attribute within the <contact> element belonging to this UE set to "terminated".

When all UE's public user identities are registered via a single P-CSCF and the subscription dialog to the reg event package of the UE is set via the respective P-CSCF, the UE shall delete these security associations or TLS sessions towards the respective P-CSCF when all public user identities have been deregistered and after the server transaction (as defined in RFC 3261 [26]) pertaining to the received NOTIFY request terminates.

NOTE 3: Deleting a security association or TLS session is an internal procedure of the UE and does not involve any SIP procedures.

NOTE 4: If all the public user identities (i.e. <contact> elements) registered by this UE are deregistered and the security associations or TLS sessions have been removed, the UE considers the subscription to the reg event package terminated since the NOTIFY request was received with Subscription-State header field containing the value of "terminated".

## 5.1.2 Subscription and notification

### 5.1.2.1 Notification about multiple registered public user identities

Upon receipt of a 2xx response to the SUBSCRIBE request the UE shall maintain the generated dialog (identified by the values of the Call-ID header field, and the values of tags in To and From header fields).

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package the UE shall perform the following actions:

- if a state attribute "active", i.e. registered is received for one or more public user identities, the UE shall store the indicated public user identities as registered;
- if a state attribute "active" is received, and the UE supports GRUU (see table A.4, item A.4/53), then for each public user identity indicated in the notification that contains a <pub-gruu> element or a <temp-gruu> element or both (as defined in RFC 5628 [94]) then the UE shall store the value of those elements in association with the public user identity;
- if a state attribute "terminated", i.e. deregistered is received for one or more public user identities, the UE shall store the indicated public user identities as deregistered and shall remove any associated GRUUs.



NOTE 1: There can be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity or when S-CSCF receives a Push-Profile-Request (PPR) from the HSS (as described in 3GPP TS 29.228 [14]) changing the status of a public user identity associated with a registered implicit set from barred to non-barred. Usually these automatically or implicitly registered public user identities belong to the same service profile of the user and they might not be available within the UE. The implicitly registered public user identities can also belong to different service profiles. The here-described procedures provide a different mechanism (to the 200 (OK) response to the REGISTER request) to inform the UE about these automatically registered public user identities.

NOTE 2: RFC 5628 [94] provides guidance on the management of temporary GRUUs, utilizing information provided in the reg event notification.

### 5.1.2.2 General SUBSCRIBE requirements

If the UE receives a 503 (Service Unavailable) response to an initial SUBSCRIBE request containing a Retry-After header field, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header field contents.

## 5.1.2A Generic procedures applicable to all methods excluding the REGISTER method

### 5.1.2A.1 UE-originating case

#### 5.1.2A.1.1 General

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request using either a given contact address or to the registration flow and the associated contact address, the UE shall:

- if IMS AKA is in use as a security mechanism:
  - a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port and the respective contact address; and
  - b) include the protected server port and the respective contact address in the Via header field entry relating to the UE;
- if SIP digest without TLS is in use as a security mechanism:
  - a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the port value of an unprotected port and the contact address where the UE expects to receive subsequent mid-dialog requests; and
  - b) populate the Via header field of the request with the port value of an unprotected port and the respective contact address where the UE expects to receive responses to the request;
- if SIP digest with TLS is in use as a security mechanism:
  - a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port; and
  - b) include the protected server port in the Via header field entry relating to the UE;
- if NASS-IMS bundled authentication is in use as a security mechanism, and therefore no port is provided for subsequent SIP messages by the P-CSCF during registration, the UE shall send any request to the same port used for the initial registration as described in subclause 5.1.1.2;
- if GPRS-IMS-Bundled authentication is in use as a security mechanism, and therefore no port is provided for subsequent SIP messages by the P-CSCF during registration, the UE shall send any request to the same port used for the initial registration as described in subclause 5.1.1.2.

If SIP digest without TLS is used, the UE shall not include RFC 3329 [48] header field s in any SIP messages.

When SIP digest is in use, upon receiving a 407 (Proxy Authentication Required) response to an initial request, the originating UE shall:

- extract the digest-challenge parameters as indicated in RFC 2617 [21] from the Proxy-Authenticate header field;
- calculate the response as described in RFC 2617 [21]; and
- send a new request containing a Proxy-Authorization header field in which the header field parameters are populated as defined in RFC 2617 [21] using the calculated response.

Where a security association or TLS session exists, the UE shall discard any SIP response that is not protected by the security association or TLS session and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

In accordance with RFC 3325 [34] the UE may insert a P-Preferred-Identity header field in any initial request for a dialog or request for a standalone transaction as a hint for creation of an asserted identity (contained in the P-Asserted-Identity header field) within the IM CN subsystem.

NOTE 1: Since the S-CSCF uses the P-Asserted-Identity header field when checking whether the UE originating request matches the initial filter criteria, the P-Preferred-Identity header field inserted by the UE determines which services and applications are invoked.

When sending any initial request for a dialog or request for a standalone transaction using either a given contact address or to the registration flow and the associated contact address, the UE may include any of the following in the P-Preferred-Identity header field:

- a public user identity which has been registered by the user with the respective contact address;
- an implicitly registered public user identity returned in a registration-state event package of a NOTIFY request whose <uri> sub-element inside the <contact> sub-element of the <registration> element is the same as the contact address being used for this request and was not subsequently deregistered or that has not expired; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

NOTE 2: The temporary public user identity specified in subclause 5.1.1.1 is not a public user identity suitable for use in the P-Preferred-Identity header field.

NOTE 3: Procedures in the network require international public telecommunication numbers when telephone numbers are used in P-Preferred-Identity header field.

NOTE 4: A number of header fields can reveal information about the identity of the user. Where privacy is required, implementers should also give consideration to other header fields that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of header fields.

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the UE shall set the From header field to "Anonymous" as specified in RFC 3261 [26].

NOTE 5: The contents of the From header field are not necessarily modified by the network based on any privacy specified by the user either within the UE indication of privacy or by network subscription or network policy. Therefore the user should include the value "Anonymous" whenever privacy is explicitly required. As the user can well have privacy requirements, terminal manufacturers should not automatically derive and include values in this header field from the public user identity or other values stored in or derived from the UICC. Where the user has not expressed a preference in the configuration of the terminal implementation, the implementation should assume that privacy is required. Users that require to identify themselves, and are making calls to SIP destinations beyond the IM CN subsystem, where the destination does not implement RFC 3325 [34], will need to include a value in the From header field other than Anonymous.

The UE shall determine the public user identity to be used for this request as follows:

- 1) if a P-Preferred-Identity was included, then use that as the public user identity for this request; or
- 2) if no P-Preferred-Identity was included, then use the default public user identity for the security association or TLS session and the associated contact address as the public user identity for this request;

The UE shall not include its "+sip.instance" header field parameter in the Contact header field in its non-register requests and responses except when the request or response is guaranteed to be sent to a trusted intermediary that will remove the "+sip.instance" header field parameter prior to forwarding the request or response to the destination.

NOTE 6: Such trusted intermediaries include an AS that all such requests as part of an application or service traverse. In order to ensure that all requests or responses containing the "+sip.instance" header field parameter are forwarded via the trusted intermediary the UE needs to have first verified that the trusted intermediary is present (e.g first contacted via a registration or configuration procedure). Including the "+sip.instance" header field parameter containing an IMEI URN does not violate RFC 7254 [153] even when the UE requests privacy using RFC 3323 [33].

If this is a request for a new dialog, the Contact header field is populated as follows:

1) a contact header value which is one of:

- if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does not indicate privacy of the P-Asserted-Identity, then the UE should insert the public GRUU ("pub-gruu" header field parameter) value as specified in RFC 5627 [93]; or
- if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does indicate privacy of the P-Asserted-Identity, then the UE should insert the temporary GRUU ("temp-gruu" header field parameter) value as specified in RFC 5627 [93]; or
- otherwise, a SIP URI containing the contact address of the UE;

NOTE 7: The above items are mutually exclusive.

- 2) include an "ob" SIP URI parameter, if the UE supports multiple registrations, and the UE wants all subsequent requests in the dialog to arrive over the same flow identified by the flow token as described in RFC 5626 [92];
- 3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag, as defined in subclause 7.9.2 and RFC 3841 [56B], the ICSI value (coded as specified in subclause 7.2A.8.2) for the IMS communication service. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the terminating UE(s); and
- 4) if the request is related to an IMS application that is supported by the UE, then the UE may include in a g.3gpp.iari-ref media feature tag, as defined in subclause 7.9.3 and RFC 3841 [56B], the IARI value (coded as specified in subclause 7.2A.9.2) that is related to the IMS application and that applies for the dialog.

If this is a request within an existing dialog, and the request includes a Contact header field, then the UE should insert the previously used Contact header field.

If the UE support multiple registrations as specified in RFC 5626 [92], the UE should include option-tag "outbound" in the Supported header field.

If this is a request for a new dialog or standalone transaction and the request is related to an IMS communication service that requires the use of an ICSI then the UE:

- 1) shall include the ICSI value (coded as specified in subclause 7.2A.8.2), for the IMS communication service that is related to the request in a P-Preferred-Service header field according to RFC 6050 [121]. If a list of network supported ICSI values was received as specified in 3GPP TS 24.167 [8G], the UE shall only include an ICSI value that is in the received list;

NOTE 8: The UE only receives those ICSI values corresponding to the IMS communication services that the network provides to the user.

- 2) may include an Accept-Contact header field containing an ICSI value (coded as specified in subclause 7.2A.8.2) that is related to the request in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 if the ICSI for the IMS communication service is known. The UE may remove one or more subclasses from an ICSI when including it in an Accept-Contact header field provided that the included ICSI corresponds to an IMS communication service.

NOTE 9: If the UE includes the same ICSI values into the Accept-Contact header field and the P-Preferred-Service header field, there is a possibility that one of the involved S-CSCFs or an AS changes the ICSI value in the P-Asserted-Service header field, which results in the message including two different ICSI values (one in the P-Asserted-Service header field, changed in the network and one in the Accept-Contact header field).

If an IMS application indicates that an IARI is to be included in a request for a new dialog or standalone transaction, the UE shall include an Accept-Contact header field containing an IARI value (coded as specified in subclause 7.2A.9.2) that is related to the request in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3841 [56B].

NOTE 10: RFC 3841 [56B] allows multiple Accept-Contact header fields along with multiple Reject-Contact header fields in a SIP request, and within those header fields, expressions that include one or more logical operations based on combinations of media feature tags. Which registered UE will be contacted depends on the Accept-Contact header field and Reject-Contact header field combinations included that evaluate to a logical expression and the relative qvalues of the registered contacts for the targeted registered public user identity. There is therefore no guarantee that when multiple Accept-Contact header fields or additional Reject-Contact header field(s) along with the Accept-Contact header field containing the ICSI value or IARI value are included in a request that the request will be routed to a contact that registered the same ICSI value or IARI value. Charging and accounting is based upon the contents of the P-Asserted-Service header field and the actual media related contents of the SIP request and not the Accept-Contact header field contents or the contact reached.

NOTE 11: The UE only includes the header field parameters "require" and "explicit" in the Accept-Contact header field containing the ICSI value or IARI value if the IMS communication service absolutely requires that the terminating UE understand the IMS communication service in order to be able to accept the session. Including the header field parameters "require" and "explicit" in Accept-Contact header fields in requests which don't absolutely require that the terminating UE understand the IMS communication service in order to accept the session creates an interoperability problem for sessions which otherwise would interoperate and violates the interoperability requirements for the ICSI in 3GPP TS 23.228 [7].

After the dialog is established the UE may change the dialog capabilities (e.g. add a media or request a supplementary service) if defined for the IMS communication service as identified by the ICSI value using the same dialog. Otherwise, the UE shall initiate a new initial request to the other user.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

If resource priority in accordance with RFC 4412 [116] is required for a dialog, then the UE shall include the Resource-Priority header field in all requests associated with that dialog.

NOTE 12: The case where the UE is unaware of the requirement for resource priority because the user requested the capability as part of the dialstring falls outside the scope of this requirement. Such cases can exist and will need to be dealt with by an appropriate functional entity (e.g. P-CSCF) to process the dialstring. For certain national implementations, signalling of a Resource-Priority header field to or from a UE is not required.

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4).

NOTE 13: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs and standalone transactions. The UE shall build a list of Route header field values made out of the following, in this order:

- a) the P-CSCF URI containing the IP address or the FQDN learnt through the P-CSCF discovery procedures; and
- b) the P-CSCF port based on the security mechanism in use:
  - if IMS AKA or SIP digest with TLS is in use as a security mechanism, the protected server port learnt during the registration procedure;

- if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is in use as a security mechanism, the unprotected server port used during the registration procedure;
- c) and the values received in the Service-Route header field saved from the 200 (OK) response to the last registration or re-registration of the public user identity with associated contact address.

NOTE 14: When the UE registers multiple contact addresses, there will be a list of Service-Route headers for each contact address. When sending a request using a given contact address and the associated security associations or TLS session, the UE will use the corresponding list of Service-Route headers to construct a list of Route headers.

The UE may indicate that proxies should not fork the request by including a "no-fork" directive within the Request-Disposition header field in the request as described in RFC 3841 [56B].

If the UE receives a 1xx or 200 (OK) response to an initial request for a dialog, the response containing a P-Asserted-Identity header field set to an emergency number as specified in 3GPP TS 22.101 [1A], the UE procedures in subclause 5.1.6.10 apply.

If the UE receives a 3xx response containing a Contact header field:

- 1) if the 3xx response is a 380 (Alternative Service) response to an INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry of the Path header field value received during registration and the response contains a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2) then the UE shall select a domain in accordance with the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B], and:
  - if the CS domain is selected, the UE behavior is defined in subclause 7.1.2 of 3GPP TS 23.167 [4B] and, where appropriate, in the access technology specific annex; and
  - if the IM CN subsystem is selected, the UE shall apply the procedures in subclause 5.1.6;

NOTE 15: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

- 2) otherwise, the UE should not automatically recurse on the Contact header field without first indicating the identity of the user to which a request will be sent and obtaining authorisation of the served user.

NOTE 16: A UE can still automatically recurse on 3xx responses as part of a service if the nature of the service enables the UE to identify 3xx responses as having originated from the home network and networks trusted by the home network and the nature of the service ensures that the charging for the requests sent as a result of the 3xx response is correlated with the original request.

NOTE 17: Automatically recursing on untrusted 3xx responses opens up the UE to being redirected to premium rate URIs without the user's consent.

### 5.1.2A.1.2 Structure of Request-URI

The UE may include a SIP URI complying with RFC 3261 [26], a tel URI complying with RFC 3966 [22], a pres URI complying with RFC 3859 [179], an im URI complying with RFC 3860 [180] or a mailto URI complying with RFC 2368 [181].

The UE may use non-international formats of E.164 numbers or non-E.164 numbers, including geo-local numbers and home-local numbers and other local numbers (e.g. private number), in the Request-URI.

Local numbering information is sent in the Request-URI in initial requests or stand alone transaction, using one of the following formats:

- 1) a tel-URI, complying with RFC 3966 [22], with a local number followed by a "phone-context" tel URI parameter value.
- 2) a SIP URI, complying with RFC 3261 [26], with the "user" SIP URI parameter set to "phone"

- 3) a SIP URI, complying with RFC 3261 [26] and RFC 4967 [103], with the "user" SIP URI parameter set to "dialstring"

The actual value of the URI depends on whether user equipment performs an analysis of the dial string input by the end user or not.

### 5.1.2A.1.3 UE without dial string processing capabilities

In this case the UE does not perform any analysis of the dial string. This requires that the dialling plan is designed so it enables the network to differentiate local numbers from other numbers.

The dial string is sent to the network, in the Request-URI of a initial request or a stand alone transaction, using one of the following formats:

- 1) a tel-URI, syntactically complying with RFC 3966 [22], with the dial string encoded as a local number followed by a "phone-context" tel URI parameter value;

EXAMPLE: tel:<input dial string>;phone-context=operator.com

- 2) a SIP URI, syntactically complying with RFC 3261 [26], with the user =phone parameter, embedding a tel-URI with a "phone-context" tel URI parameter value;

EXAMPLE: sip:<input dial string>;  
phone-context=operator.com@operator.com;user=phone

- 3) a SIP URI, complying with RFC 3261 [26] and RFC 4967 [103], with the user=dialstring parameter and a with a "phone-context" tel-URI parameter value in the user part; or

EXAMPLE: sip:<input dial string>;  
phone-context=operator.com@operator.com;user=dialstring

- 4) a SIP URI syntactically complying with RFC 3261 [26], where the user part contains the dial string and the domain name is specific enough to enable to network to understand that the user part contains a dial string.

EXAMPLE: sip:<input dial string>@dialstrings.entreprise.com

For cases 1), 2), and 3) the UE shall set the "phone-context" tel URI parameter in accordance with subclause 5.1.2A.1.5.

### 5.1.2A.1.4 UE with dial string processing capabilities

In this case the UE performs sufficient dial string analysis (or receives an explicit indication from the user) to identify the type of numbering that is used and processes the dial string accordingly before building the Request-URI.

If the UE detects that a local dialling plan is being used, where the terminal is able to identify a global telephone number, the normal procedures apply after removing all dial string elements used for local numbering detection purposes (e.g. escape codes).

If the UE detects that a local (private or public) dialling plan is being used, it may decide to send the dial string unchanged to the network as described in subclause 5.1.2A.1.3 or the UE may decide to alter it to comply with the local numbering plan (e.g. remove all dial string elements used for local numbering detection).

In the latter case the local numbering information is sent using one of the following formats:

- 1) a tel-URI, complying with RFC 3966 [22], with a local number followed by a "phone-context" tel-URI parameter value;
- 2) a SIP URI, complying with RFC 3261 [26], with the "user" SIP URI parameter set to "phone" and a user part embedding a local number with a phone-context parameter; and
- 3) if the UE intends to send information related to supplementary services, a SIP URI, complying with RFC 3261 [26] and RFC 4967 [103], with the "user" SIP URI parameter set to "dialstring" and a with a "phone-context" tel URI parameter value in the user part.

The UE shall set the "phone-context" tel URI parameter in accordance with subclause 5.1.2A.1.5.

NOTE: The way how the UE process the dial-string and handles special characters (e.g. pause) in order to produce a conformant SIP URI or tel-URI according to RFC 3966 [22] is implementation specific.

As a general rule, recognition of special service numbers shall take priority over other dialling plan issues. If the dial string equates to a pre-configured service URN as specified in RFC 5031 [69]) then the service-urn should be sent.

#### 5.1.2A.1.5 Setting the "phone-context" tel URI parameter

When the UE uses home-local number, the UE shall include in the "phone-context" tel URI parameter the home domain name in accordance with RFC 3966 [22].

When the UE uses geo-local number, the UE shall:

- if access technology information available to the UE (i.e., the UE can insert P-Access-Network-Info header field into the request), include the access technology information in the "phone-context" tel URI parameter according to RFC 3966 [22] as defined in subclause 7.2A.10; and
- if access technology information is not available to the UE (i.e., the UE cannot insert P-Access-Network-Info header field into the request), include in the "phone-context" tel URI parameter the home domain name prefixed by the "geo-local." string according to RFC 3966 [22] as defined in subclause 7.2A.10.

When the UE uses other local numbers, than geo-local number or home local numbers, e.g. private numbers that are different from home-local number or the UE is unable to determine the type of the dialled number, the UE shall include a "phone-context" tel URI parameter set according to RFC 3966 [22], e.g. if private numbers are used a domain name to which the private addressing plan is associated.

NOTE 1: The "phone-context" tel URI parameter value can be entered or selected by the subscriber, or can be a "pre-configured" value (e.g. using OMA-DM with the management object specified in 3GPP TS 24.167 [8G]) inserted by the UE.

NOTE 2: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is implementation specific.

NOTE 3: Home operator's local policy can define a prefix string(s) to enable subscribers to differentiate dialling a geo-local number and/or a home-local number.

#### 5.1.2A.1.6 Abnormal cases

In the event the UE receives a 504 (Server Time-out) response containing:

- 1) a P-Asserted-Identity header field set to a value equal to a URI:
  - a) from the Service-Route header field value received during registration; or
  - b) from the Path header field value received during registration; and

NOTE 1: If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field and Service-Route header field values. The Path header field value and Service-Route header field value corresponding to the flow on which the 504 (Server Time-out) response was received are checked.

- 2) a Content-Type header field set according to subclause 7.6 (i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field, independent of the value or presence of Content-Disposition parameters, then the following treatment is applied:
  - a) if the 504 (Server Time-out) response includes an IM CN subsystem XML body as described in subclause 7.6 with the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element:
    - A) with the <type> child element set to "restoration" (see table 7.6.2); and
    - B) with the <action> child element set to "initial-registration" (see table 7.6.3);

then the UE:

- shall initiate S-CSCF restoration procedures by performing an initial registration as specified in subclause 5.1.1.2; and

- may provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element.

NOTE 2: If the UE has discovered multiple P-CSCF addresses and has information that the P-CSCF was unable to forward the request resulting in sending back the 504 (Server Time-out) response, when starting the initial registration it is appropriate for the UE to select a P-CSCF address different from the one used for the registration binding on which the 504 (Server Time-out) response was received.

When sending a request from a contact address (or via a registration flow if the multiple registration mechanism is used) which is bound to a public user identity by registration which used a P-CSCF address, and:

- if timer F expires in the "Trying" state of non-INVITE client transaction as described in IETF RFC 3261 [26];
- if a fatal transport error is reported by the transport layer in the "Trying" state of non-INVITE client transaction as described in IETF RFC 3261 [26];
- if timer B expires in the "Calling" state of INVITE client transaction as described in IETF RFC 6026 [163]; or
- if a fatal transport error is reported by the transport layer in "Calling" state of INVITE client transaction as described in IETF RFC 6026 [163];

Then the UE shall:

- 1) if the multiple registration mechanism is not used:
  - A) consider the contact address as not bound to any public user identity;
  - B) remove the P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1; and
  - C) initiate an initial registration as specified in subclause 5.1.1.2 using a P-CSCF different than the P-CSCF using which the contact address was registered; and
- 2) if the multiple registration mechanism is used, declare the registration flow dead as defined in RFC 5626 [92] and remove the P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1.

NOTE 3: When a fatal transport error occurs, further steps might be necessary to restore the transport layer, possibly including re-establishment of an IP-CAN bearer.

### 5.1.2A.2 UE-terminating case

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

Where a security association or TLS session exists, the UE shall discard any SIP request that is not protected by the security association or TLS session and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

If an initial request contains an Accept-Contact header field containing the g.3gpp.icsi-ref media feature tag with an ICSI value, the UE should invoke the IMS application that is the best match for the ICSI value.

If an initial request contains an Accept-Contact header field containing the g.3gpp.iari-ref media feature tag with an IARI value the UE should invoke the IMS application that is the best match for the IARI value.

The UE can receive multiple ICSI values, IARI values or both in an Accept-Contact header field. In this case it is up to the implementation which of the multiple ICSI values or IARI values the UE takes action on.

NOTE 1: The application verifies that the contents of the request (e.g. SDP media capabilities, Content-Type header field) are consistent with the the ICSI value in the g.3gpp.icsi-ref media feature tag and IARI value contained in the g.3gpp.iari-ref media feature tag.

If an initial request does not contain an Accept-Contact header field containing a g.3gpp.icsi-ref media feature tag or a g.3gpp.iari-ref media feature tag the UE shall invoke the application that is the best match based on the contents of the request (e.g. SDP media capabilities, Content-Type header field, media feature tag).



The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

NOTE 2: In the UE-terminating case, this version of the document makes no provision for the UE to provide a P-Preferred-Identity in the form of a hint.

NOTE 3: A number of header fields can reveal information about the identity of the user. Where, privacy is required, implementers should also give consideration to other header fields that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of header fields.

The UE shall not include its "+sip.instance" header field parameter in the Contact header field in its non-register requests and responses except when the request or response is guaranteed to be sent to a trusted intermediary that will remove the "+sip.instance" header field parameter prior to forwarding the request or response to the destination.

NOTE 4: Such trusted intermediaries include an AS that all such requests as part of an application or service traverse. In order to ensure that all requests or responses containing the "+sip.instance" header field parameter are forwarded via the trusted intermediary the UE needs to have first verified that the trusted intermediary is present (e.g first contacted via a registration or configuration procedure). Including the "+sip.instance" header field parameter containing an IMEI URN does not violate RFC 7254 [153] even when the UE requests privacy using RFC 3323 [33].

If the response includes a Contact header field, and the response is sent within an existing dialog, and the Contact address previously used in the dialog was a GRUU, then the UE should insert the previously used GRUU value in the Contact header field as specified in RFC 5627 [93].

If the response includes a Contact header field, and the response is not sent within an existing dialog, the Contact header field is populated as follows:

- 1) if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity from the P-Called-Party-ID header field, and the UE does not indicate privacy of the contents of the P-Asserted-Identity header field, then the UE should insert the public GRUU ("pub-gruu" header field parameter) value as specified in RFC 5627 [93];
- 2) if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity from the P-Called-Party-ID header field, and the UE does indicate privacy of the P-Asserted-Identity, then should insert the temporary GRUU ("temp-gruu" header field parameter) value in the Contact header field as specified in RFC 5627 [93];

NOTE 5: The above items 1 and 2 are mutually exclusive.

- 3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3841 [56B] the ICSI value (coded as specified in subclause 7.2A.8.2), for the IMS communication service and then the UE may include the IARI value for any IMS application that applies for the dialog, (coded as specified in subclause 7.2A.9.2), that is related to the request in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3841 [56B]. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the originating UE(s) and other IARI values for the IMS application that is related to the IMS communication service; and
- 4) if the request is related to an IMS application that is supported by the UE when the use of an ICSI is not needed, then the UE may include the IARI value (coded as specified in subclause 7.2A.9.2), that is related to any IMS application and that applies for the dialog, in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3841 [56B].

After the dialog is established the UE may change the dialog capabilities (e.g. add a media or request a supplementary service) if defined for the IMS communication service as identified by the ICSI value using the same dialog. Otherwise, the UE shall initiate a new initial request to the other user.

If the UE did not insert a GRUU in the Contact header field then the UE shall include a port in the address in the Contact header field as follows:

- if IMS AKA or SIP digest with TLS is being used as a security mechanism, the protected server port value as in the initial registration; or

- if SIP digest without TLS is being used as a security mechanism, the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests. The UE shall set the unprotected port value to the port value used in the initial registration.

If the UE receives a Resource-Priority header field in accordance with RFC 4412 [16] in an initial request for a dialog, then the UE shall include the Resource-Priority header field in all requests associated with that dialog.

NOTE 6: For certain national implementations, signalling of a Resource-Priority header field to and from a UE is not required.

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any response to a request for a dialog, any subsequent request (except CANCEL requests) or response (except CANCEL responses) within a dialog or any response to a standalone method (see subclause 7.2A.4).

## 5.1.3 Call initiation - UE-originating case

### 5.1.3.1 Initial INVITE request

Where multiple domains exist for initiating a call/session, before sending an initial INVITE request, the UE shall perform access domain selection in accordance with the appropriate specification for the IP-CAN in use, taking into account the media to be requested. Access domain selection allows the policy of the network operator to be taken into account before an INVITE request is sent. Access dependent aspects of access domain selection are defined in the access technology specific annexes for each access technology.

Upon generating an initial INVITE request, the UE shall include the Accept header field with "application/sdp", the MIME type associated with the 3GPP IM CN subsystem XML body (see subclause 7.6.1) and any other MIME type the UE is willing and capable to accept.

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 [30] as updated by RFC 4032 [64].

The preconditions mechanism should be supported by the originating UE.

The UE may initiate a session without the precondition mechanism if the originating UE does not require local resource reservation.

NOTE 1: The originating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

In order to allow the peer entity to reserve its required resources, an originating UE supporting the precondition mechanism should make use of the precondition mechanism, even if it does not require local resource reservation.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header field mechanism;and
- indicate the support for the preconditions mechanism and specify it using the Supported header field mechanism.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall not indicate the requirement for the precondition mechanism by using the Require header field mechanism.

NOTE 2: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26]. The UE can accept or reject any of the forked responses, for example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs.

Upon successful reservation of local resources the UE shall confirm the successful resource reservation (see subclause 6.1.2) within the next SIP request.

NOTE 3: In case of the precondition mechanism being used on both sides, this confirmation will be sent in either a PRACK request or an UPDATE request. In case of the precondition mechanism not being supported on one or both sides, alternatively a reINVITE request can be used for this confirmation after a 200 (OK) response has been received for the initial INVITE request, in case the terminating UE does not support the PRACK request (as described in RFC 3262 [27]) and does not support the UPDATE request (as described in RFC 3311 [29]).

NOTE 4: If the UE supports the P-Early-Media header field, upon receiving a 18x provisional response with a P-Early-Media header field indicating authorized early media, as described in RFC 5009 [109], if the preconditions are met, the UE should, based on local configuration, present received early media to the user.

NOTE 5: If the UE supports the P-Early-Media header field, upon receiving a 180 (Ringing) provisional response with a P-Early-Media header field indicating authorized early media, as described in RFC 5009 [109], if the preconditions are met, and the UE presents the received early media to the user based on local configuration, the UE will not provide an indication that the invited user is being alerted.

NOTE 6: If the UE supports the P-Early-Media header field and if the most recently received P-Early-Media header field within the dialog includes a parameter applicable to media stream with value "inactive", then based on local configuration, the UE will provide an indication that the invited user is being alerted and stop presenting received early media to the user if requested by any previous receipt of P-Early-Media header field within the dialog.

If the UE wishes to receive early media authorization indications, as described in RFC 5009 [109], the UE shall add the P-Early-Media header field with the "supported" parameter to the INVITE request.

To request end to access edge media security on a media level, the UE shall send an SDP Offer for an SRTP stream containing one or more SDES crypto attributes, each with a key and other security context parameters required according to RFC 4568 [168], together with the attribute "a=3ge2ae".

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall not progress any remaining early dialogues to established dialogs. Therefore, upon the reception of a subsequent final 200 (OK) response for an INVITE request (e.g., due to forking), the UE shall:

- 1) acknowledge the response with an ACK request; and
- 2) send a BYE request to this dialog in order to terminate it.

Upon receiving a 488 (Not Acceptable Here) response to an initial INVITE request, the originating UE should send a new INVITE request containing SDP according to the procedures defined in subclause 6.1.

NOTE 7: An example of where a new request would not be sent is where knowledge exists within the UE, or interaction occurs with the user, such that it is known that the resulting SDP would describe a session that did not meet the user requirements.

Upon receiving a 421 (Extension Required) response to an initial INVITE request in which the precondition mechanism was not used, including the "precondition" option-tag in the Require header field, the originating UE shall:

- send a new INVITE request using the precondition mechanism, if the originating UE supports the precondition mechanism; and
- send an UPDATE request as soon as the necessary resources are available and a 200 (OK) response for the first PRACK request has been received.

Upon receiving a 503 (Service Unavailable) response to an initial INVITE request containing a Retry-After header field, then the originating UE shall not automatically reattempt the request until after the period indicated by the Retry-After header field contents.

The UE may include a "cic" tel-URI parameter in a tel-URI, or in the userinfo part of a SIP URI with user=phone, in the Request-URI of an initial INVITE request if the UE wants to identify a user-dialed carrier, as described in RFC 4694 [112].

NOTE 8: The method whereby the UE determines when to include a "cic" tel-URI parameter and what value it should contain is outside the scope of this document (e.g. the UE could use a locally configured digit map to look for special prefix digits that indicate the user has dialled a carrier).

NOTE 9: The value of the "cic" tel-URI parameter reported by the UE is not dependent on UE location (e.g. the reported value is not affected by roaming scenarios).

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry of the Path header field value received during registration and the the response containing a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2), the UE shall select a domain in accordance with the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B], and:

- if the CS domain is selected, the UE behavior is defined in subclause 7.1.2 of 3GPP TS 23.167 [4B] and, where appropriate, in the access technology specific annex; and
- if the IM CN subsystem is selected, the UE shall apply the procedures in subclause 5.1.6.

NOTE 10: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

Upon receiving a 199 (Early Dialog Terminated) provisional response to an established early dialog the UE shall release resources specifically related to that early dialog.

## 5.1.4 Call initiation - UE-terminating case

### 5.1.4.1 Initial INVITE request

The preconditions mechanism should be supported by the terminating UE.

The handling of incoming initial INVITE requests at the terminating UE is mainly dependent on the following conditions:

- the specific service requirements for "integration of resource management and SIP" extension (hereafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30] as updated by RFC 4032 [64], and with the request for such a mechanism known as a precondition); and
- the UEs configuration for the case when the specific service does not require the precondition mechanism.

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

- a) the received INVITE request includes the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header field with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or
- b) the received INVITE request does not include the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall not make use of the precondition mechanism.

If local resource reservation is not required by the terminating UE and the terminating UE supports the precondition mechanism and:

- a) the received INVITE request includes the "precondition" option-tag in the Supported header field and:
  - the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism; or

- the required local resources at the originating UE and the terminating UE are available, the terminating UE may use the precondition mechanism;
- b) the received INVITE request does not include the "precondition" option-tag in the Supported header field or Require header field, the terminating UE shall not make use of the precondition mechanism; or
- c) the received INVITE request includes the "precondition" option-tag in the Require header field, the terminating UE shall use the precondition mechanism.

NOTE 2: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26].

NOTE 3: If the terminating UE does not support the precondition mechanism it will apply regular SIP session initiation procedures.

If the terminating UE requires a reliable alerting indication at the originating side, the UE shall send the 180 (Ringing) response reliably. If the received INVITE request indicated support for reliable provisionable responses, but did not require their use, the terminating UE shall send provisional responses reliably only if the provisional response carries SDP or for other application related purposes that requires its reliable transport.

NOTE 4: Certain applications, services and operator policies might mandate the terminating UE to send a 199 (Early Dialog Terminated) provisional response (see RFC 6228 [142]) prior to sending a non-2xx final response to the INVITE request.

If the terminating UE uses the precondition mechanism, upon successful reservation of local resources:

- if the originating side requested confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE, the terminating UE shall confirm the successful resource reservation (see subclause 6.1.3) within an SIP UPDATE request; and

NOTE 5: Originating side requests confirmation for the result of the resource reservation at the terminating UE e.g. when an application server performs 3rd party call control. The request for confirmation for the result of the resource reservation at the terminating UE can be included e.g. in the SDP answer in the PRACK request.

- if the originating side did not request confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE, the terminating UE shall not confirm the successful resource reservation (see subclause 6.1.3) within an UPDATE request.

NOTE 6: The terminating UE can send an UPDATE request for reasons other than confirmation of the successful resource reservation.

If the terminating UE included an SDP offer or an SDP answer in a reliable provisional response to the INVITE request and both the terminating UE and the originating UE support UPDATE method, then in order to remove one or more media streams negotiated in the session for which a final response to the INVITE request has not been sent yet, the terminating UE sends an UPDATE request with a new SDP offer and delays sending of 200 (OK) response to the INVITE request till after reception of 200 (OK) response to the UPDATE request.

## 5.1.5 Call release

Void.

## 5.1.6 Emergency service

### 5.1.6.1 General

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN does not define emergency bearers, the UE shall attempt an emergency call as described in subclause 5.1.6.8.4.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN defines emergency bearers and the core network has indicated that it supports emergency bearers, the UE shall:

- 1) perform an initial emergency registration, as described in subclause 5.1.6.2; and
- 2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is not currently registered, the UE shall:

- 1) perform an initial emergency registration, as described in subclause 5.1.6.2; and
- 2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is attached to a different network than its home operator's network (e.g. VPLMN), the UE shall:

- 1) perform an initial emergency registration, as described in subclause 5.1.6.2; and
- 2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE has no credentials the UE can make an emergency call without being registered. The UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

The IP-CAN can, dependent on the IP-CAN capabilities, provide local emergency numbers (including information about emergency service categories) to the UE which has that capability, in order for the UE to recognize these numbers as emergency call.

### 5.1.6.2 Initial emergency registration

When the user initiates an emergency call, if emergency registration is needed (including cases described in subclause 5.1.6.2A), the UE shall perform an emergency registration prior to sending the SIP request related to the emergency call.

The UE shall have only one valid emergency registration at any given time. If the UE initiates a new emergency registration using different contact address, and the previous emergency registration has not expired, the UE shall consider the previous emergency registration as expired.

IP-CAN procedures for emergency registration are defined in 3GPP TS 23.167 [4B] and in each access technology specific annex.

When a UE performs an initial emergency registration the UE shall perform the actions as specified in subclause 5.1.1.2 with the following additions and modifications:

- a) the UE shall include a "sos" SIP URI parameter in the Contact header field as described in subclause 7.2A.13, indicating that this is an emergency registration and that the associated contact address is allowed only for emergency service; and
- b) the UE shall populate the From and To header fields of the REGISTER request with:
  - the first entry in the list of public user identities provisioned in the UE;
  - the default public user identity obtained during the normal registration, if the UE is not provisioned with a list of public user identities, but the UE is currently registered to the IM CN subsystem; and
  - the derived temporary public user identity, in all other cases.

When the UE performs an initial emergency registration and whilst this emergency registration is active, the UE shall:

- handle the emergency registration independently from any other ongoing registration to the IM CN subsystem;

- handle any signalling or media related IP-CAN for the purpose of emergency calls independently from any other established IP-CAN for IM CN subsystem related signalling or media; and
- handle all SIP signalling and all media related to the emergency call independently from any other ongoing IM CN subsystem signalling and media.

#### 5.1.6.2A New initial emergency registration

The UE shall perform a new initial emergency registration, as specified in subclause 5.1.6.2, if the UE determines that:

- it has previously performed an emergency registration which has not yet expired; and
- it has obtained an IP address from the serving IP-CAN, as specified in subclause 9.2.1, different than the IP address used for the emergency registration.

#### 5.1.6.3 Initial subscription to the registration-state event package

Upon receiving the 200 (OK) to the REGISTER request that completes the emergency registration, the UE shall not subscribe to the reg event package of the public user identity specified in the REGISTER request.

#### 5.1.6.4 User-initiated emergency reregistration

The UE shall perform user-initiated emergency reregistration as specified in subclause 5.1.1.4 if half of the time for the emergency registration has expired and:

- the UE has emergency related ongoing dialog; or
- standalone transactions exist; or
- the user initiates an emergency call.

The UE shall not perform user-initiated emergency reregistration in any other cases.

#### 5.1.6.5 Authentication

When a UE performs authentication a UE shall perform the procedures as specified in subclause 5.1.1.5.

#### 5.1.6.6 User-initiated emergency deregistration

Once the UE registers a public user identity and an associated contact address via emergency registration, the UE shall not perform user-initiated deregistration of the respective public user identity and the associated contact address.

NOTE: The UE will be deregistered when the emergency registration expires.

#### 5.1.6.7 Network-initiated emergency deregistration

An emergency registration will not be deregistered by the network (see subclause 5.4.8.4).

#### 5.1.6.8 Emergency session setup

##### 5.1.6.8.1 General

The UE shall translate any user indicated emergency number as specified in 3GPP TS 22.101 [1A] to an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69].

When an initial request for a dialog or a standalone transaction, or an unknown method transmitted as part of UE detected emergency call procedures as defined in subclause 5.1.6 is initiated:

- in event other than reception of a 380 (Alternative Service) response to an initial request for a dialog, or a standalone transaction, or an unknown method as defined in procedures in subclause 5.1.2A.1.1, subclause 5.1.3.1, subclause 5.1.6.8.1, subclause 5.1.6.8.3 and subclause 5.1.6.8.4; or
- upon reception of a 380 (Alternative Service) response to an initial request for a dialog, or a standalone transaction, or an unknown method as defined in procedures in subclause 5.1.2A.1.1, subclause 5.1.3.1, subclause 5.1.6.8.1, subclause 5.1.6.8.3 and subclause 5.1.6.8.4, and the 380 (Alternative Service) response does not contain a Contact header field containing a service URN with a top-level service type of "sos";

the Request-URI of the initial request for a dialog or the standalone transaction, or the unknown method transmitted as part of UE detected emergency call procedures as defined in subclause 5.1.6 shall include one of the following service URNs; "urn:service:sos", "urn:service:sos.ambulance", "urn:service:sos.police", "urn:service:sos.fire", "urn:service:sos.marine", "urn:service:sos.mountain". If the UE can determine the type of emergency service the UE shall use an emergency service URN with a sub-service type corresponding to the type of emergency service.

NOTE 1: A service URN with a top-level service type of "sos" is used only when the user intends to establish an emergency call.

When an initial request for a dialog or a standalone transaction, or an unknown method transmitted as part of UE detected emergency call procedures as defined in subclause 5.1.6 is initiated upon reception of 380 (Alternative Service) response to an initial request for a dialog, or a standalone transaction, or an unknown method as defined in procedures in subclause 5.1.2A.1.1, subclause 5.1.3.1, subclause 5.1.6.8.1, subclause 5.1.6.8.3 and subclause 5.1.6.8.4, and if the 380 (Alternative Service) response contains a Contact header field containing a service URN with a top-level service type of "sos", the UE shall set the Request-URI of the initial request for a dialog or the standalone transaction, or the unknown method transmitted as part of UE detected emergency call procedures as defined in subclause 5.1.6 to the service URN of the Contact header field of the 380 (Alternative Service) response.

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response including a 3GPP IM CN subsystem XML body as described in subclause 7.6 that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2), the UE shall automatically send an ACK request to the P-CSCF as per normal SIP procedures and terminate the session. In addition, if the 380 (Alternative Service) response includes a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration:

- the UE may also provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element; and
- one of subclause 5.1.6.8.3 or subclause 5.1.6.8.4 applies.

NOTE 2: Emergency numbers which the UE does not detect, will be treated as a normal call.

NOTE 3: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

#### 5.1.6.8.2 Emergency session set-up in case of no registration

When establishing an emergency session for an unregistered user, the UE is allowed to receive responses to emergency requests and requests inside an established emergency session on the unprotected ports. The UE shall reject or silently discard all other messages not arriving on a protected port. Additionally, the UE shall transmit signalling packets pertaining to the emergency session from the same IP address and unprotected port on which it expects to receive signalling packets containing the responses to emergency requests and the requests inside the established emergency session.

Prior to establishing an emergency session for an unregistered user, the UE shall acquire a local IP address, discover a P-CSCF, and establish an IP-CAN bearer that can be used for SIP signalling. The UE shall send only the initial INVITE requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial INVITE request to the SIP default port values as specified in RFC 3261 [26].

The UE shall apply the procedures as specified in subclause 5.1.2A.1 and subclause 5.1.3 with the following additions:

- 1) the UE shall set the From header field of the INVITE request to "Anonymous" as specified in RFC 3261 [26];
- 2) the UE shall include a service URN in the Request-URI of the initial INVITE request in accordance with subclause 5.1.6.8.1;

NOTE 1: Other specifications make provision for emergency service identifiers, that are not specifically the emergency service URN, to be recognised in the UE. Emergency service identifiers which the UE does not detect will be treated as a normal call by the UE.



- 3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;
- 4) if available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall include in the P-Access-Network-Info header field in any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request. The UE shall populate the P-Access-Network-Info header field with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4). The P-Access-Network-Info header field contains the location identifier such as the cell id, the line id or the identity of the I-WLAN access node, which is relevant for routing the emergency call;
- 5) if defined by the access technology specific annex, the UE shall populate the P-Preferred-Identity header field in the INVITE request with an equipment identifier as a SIP URI. The special details of the equipment identifier to use depend on the IP-CAN;
- 6) a Contact header field set to include SIP URI that contains in the hostport parameter the IP address of the UE and an unprotected port where the UE will receive incoming requests belonging to this dialog. The UE shall also include a "sip.instance" media feature tag containing Instance ID as described in RFC 5626 [92]. The UE shall not include either the public or temporary GRUU in the Contact header field;
- 7) a Via header field set to include the IP address of the UE in the sent-by field and for the UDP the unprotected server port value where the UE will receive response to the emergency request, while for the TCP, the response is received on the TCP connection on which the emergency request was sent. The UE shall also include "rport" header field parameter with no value in the top Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with, and during the lifetime of, the emergency session, as described in RFC 6223 [143];

NOTE 2: The UE inserts the same IP address and port number into the Contact header field and the Via header field, and sends all IP packets to the P-CSCF from this IP address and port number.

- 8) if the UE has its location information available, or a URI that points to the location information, the UE shall include a Geolocation header field in the INVITE request in the following way:
  - if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442 [89]; or
  - if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119 [90], include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442 [89];
- 9) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89]; and
- 10) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is inapplicable in this area.

NOTE 5: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs. The UE shall build a Route header field value containing only the P-CSCF URI (containing the unprotected port number and the IP address or the FQDN learnt through the P-CSCF discovery procedures).

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause 5.1.1.4.

NOTE 6: It is an implementation option whether these actions are also triggered by other means.

NOTE 7: A number of header fields can reveal information about the identity of the user. Where privacy is required, implementers should also give consideration to other header fields that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of header fields.

NOTE 8: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

If the response for the initial INVITE request indicates that the UE is behind NAT, and the INVITE request was sent over TCP connection, the UE shall keep the TCP connection during the entire duration of the emergency session. In this case the UE will receive all responses to the emergency requests and the requests inside the established emergency session over this TCP connection.

If the Via header field of any provisional response, or of the final 200 (OK) response, for the initial INVITE request contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, the UE shall start to send keep-alives associated with the session towards the P-CSCF, as described in RFC 6223 [143].

#### 5.1.6.8.3 Emergency session set-up within an emergency registration

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A and 5.1.3 with the following additions:

- 1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;
- 2) the UE shall include a service URN in the Request-URI of the INVITE request in accordance with subclause 5.1.6.8.1;
- 3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;
- 4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routing the IMS emergency call;

NOTE 1: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

- 5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 2: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

- 6) void;
- 7) if the UE has its location information available, or a URI that points to the location information, then the UE shall include a Geolocation header field in the INVITE request in the following way:
  - if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442 [89]; or
  - if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119 [90], include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442 [89];
- 8) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89]; and

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

- 9) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

NOTE 4: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

In the event the UE receives a 380 (Alternative Service) response with a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration, and the Content-Type header field set according to subclause 7.6 (i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field, independent of the value or presence of Content-Disposition parameters, then the following treatment is applied:

- 1) if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2), then the UE shall:
  - a) if the CS domain is available to the UE, and no prior attempt using the CS domain for the current emergency call attempt has been made, attempt emergency call via CS domain using appropriate access technology specific procedures;
  - b) if the CS domain is not available to the UE or the emergency call has already been attempted using the CS domain, then perform one of the following actions:
    - if the <action> child element of the <alternative-service> child element of the <ims-3gpp> element in the IM CN subsystem XML body as described in subclause 7.6 is set to "emergency-registration" (see table 7.6.3), perform an initial emergency registration using a different VPLMN if available, as described in subclause 5.1.6.2 and if the new emergency registration succeeded, attempt an emergency call as described in this subclause; or
    - perform implementation specific actions to establish the emergency call; and
- 2) if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 with the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2) then the UE may also provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element.

NOTE 5: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

#### 5.1.6.8.4 Emergency session setup within a non-emergency registration

The UE shall apply the procedures as specified in subclauses 5.1.2A and 5.1.3 with the following additions:

- 1) the UE shall include a service URN in the Request-URI of the INVITE request in accordance with subclause 5.1.6.8.1;
- 2) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;
- 3) the UE shall insert in the INVITE request, a From header field that includes the public user identity or the tel URI associated with the public user identity, as described in subclause 4.2;
- 4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the UE shall insert in the P-Access-Network-Info header field a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routing the IMS emergency call;

NOTE 1: 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

- 5) the UE shall insert in the INVITE request one or two P-Preferred-Identity header field(s) that include the public user identity or the tel URI associated with the public user identity as described in subclause 4.2;

NOTE 2: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

- 6) if the UE has its location information available, or a URI that points to the location information, then the UE shall include a Geolocation header field in the INVITE request in the following way:
- if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442 [89]; or
  - if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119 [90], include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442 [89];
- 7) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89];
- 8) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request; and

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

- 9) if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, then insert the public GRUU ("pub-gruu" header field parameter) value in the Contact header field as specified in RFC 5627 [93]. Otherwise the UE shall include the address in the Contact header field set to contain the IP address or FQDN of the UE, and the UE shall also include:
- if IMS AKA or SIP digest with TLS is being used as a security mechanism, the protected server port value as in the initial registration; or
  - if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled Authentication is being used as a security mechanism, the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests. The UE shall set the unprotected port value to the port value used in the initial registration.

In the event the UE receives a 380 (Alternative Service) response with a P-Asserted-Identity header field with a value equal to the value of the SIP URI of the P-CSCF received in the Path header field during registration, and the Content-Type header field set according to subclause 7.6 (i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field, independent of the value or presence of Content-Disposition parameters, then the following treatment is applied:

- a) if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 with an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2), then the UE shall:
- if the <action> child element of the <alternative-service> child element of the <ims-3gpp> element in the IM CN subsystem XML body as described in subclause 7.6 is set to "emergency-registration" (see table 7.6.3), perform an initial emergency registration, as described in subclause 5.1.6.2 and attempt an emergency call as described in subclause 5.1.6.8.3;
  - attempt emergency call via CS domain using appropriate access technology specific procedures, if available and not already tried; or
  - perform implementation specific actions to establish the emergency call; and

- b) if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 with an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.6.2) then the UE may also provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element.

NOTE 4: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

NOTE 5: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

### 5.1.6.9 Emergency session release

Normal call release procedure shall apply, as specified in the subclause 5.1.5.

#### 5.1.6.10 Successful or provisional response to a request not detected by the UE as relating to an emergency session

If the UE receives a 1xx or 200 (OK) response to an initial request for a dialog, the response containing a P-Asserted-Identity header field set to an emergency number as specified in 3GPP TS 22.101 [1A], and:

- if a public GRUU value (pub-gruu) has been saved associated with the public user identity, the public GRUU value has not been included in the Contact header field of the initial request for a dialog as specified in RFC 5627 [93];
- if a public GRUU value (pub-gruu) has not been saved and a protected server port was not included in the address in the Contact header field of the the initial request for a dialog; or
- if the UE has its geographical location information available, or a URI that points to the location information, and the geographical location information or URI has not been included in the initial request for a dialog; then the UE shall send an UPDATE request according to RFC 3311 [29]; and
  - 1) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the UE shall include in the UPDATE request a P-Access-Network-Info header field and it shall contain a location identifier such as the cell id or the identity of the I-WLAN access node;
  - 2) if the UE has its geographical location information available, or a URI that points to the location information, then the UE shall include it in the UPDATE request in the following way:
    - I) if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442 [89]; or
    - II) if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119 [90], include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442 [89];
  - 3) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89];
  - 4) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request; and
  - 5) if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity, then the UE shall insert the public GRUU ("pub-gruu" header field parameter) value in the Contact header field of the UPDATE request as specified in RFC 5627 [93]; otherwise the UE shall include the address in the Contact header field set in accordance with subclause 5.1.6.8.4, item 8.

NOTE 1: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

NOTE 2: It is suggested that UEs only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

NOTE 3: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

NOTE 4: In this version of the specification, only requests creating a dialog can request emergency services.

If the UE receives a 1xx or 200 (OK) response to an initial request for a dialog the response containing a P-Asserted-Identity header field set to an emergency number as specified in 3GPP TS 22.101 [1A], then the UE may indicate the nature of the session to the user.

### 5.1.7 Void

### 5.1.8 Void

## 5.2 Procedures at the P-CSCF

### 5.2.1 General

Where the P-CSCF provides emergency call support, the procedures of subclause 5.2.10 shall be applied first.

Subclause 5.2.2 through subclause 5.2.9 define P-CSCF procedures for SIP that do not relate to emergency. All SIP requests are first screened according to the procedures of subclause 5.2.10 to see if they do relate to an emergency.

For all SIP transactions identified:

- as relating to an emergency; or
- if priority is supported, as containing an authorised Resource-Priority header field or a temporarily authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the P-CSCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs. If the P-CSCF recognises the need for priority processing to a request or if the P-CSCF recognises the need to provide different priority processing than the one indicated by the originating UE, based on the information stored during registration, the P-CSCF may insert or modify Resource-Priority header in accordance with RFC 4412 [116].

NOTE 1: The special treatment can include filtering, higher priority processing, routing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

The P-CSCF shall support the Path and Service-Route header fields.

NOTE 2: The Path header field is only applicable to the REGISTER request and its 200 (OK) response. The Service-Route header field is only applicable to the 200 (OK) response of REGISTER request.

NOTE 3: In subsequent procedures, the P-CSCF can address the needs of individual users (e.g. in support of attached enterprise networks or in support of priority mechanisms, from information saved during registration. In this release of the specification, no information is specified in the registration procedures to perform this, and therefore this information has to either be associated with the user at time of registration from configured information, or by a mechanism outside the scope of this release of the specification.

When the P-CSCF sends any request or response to the UE, before sending the message the P-CSCF shall:

- remove the P-Charging-Function-Addresses and P-Charging-Vector header fields, if present.

When the P-CSCF receives any request or response from the UE, the P-CSCF:

- 1) shall remove the P-Charging-Function-Addresses and P-Charging-Vector header fields, if present. Also, the P-CSCF shall ignore any data received in the P-Charging-Function-Addresses and P-Charging-Vector header fields; and
- 2) may insert previously saved values into the P-Charging-Function-Addresses and P-Charging-Vector header fields before forwarding the message;

NOTE 4: When the P-CSCF is located in the visited network, then it will not receive the P-Charging-Function-Addresses header field from the S-CSCF, IBCF, or I-CSCF. Instead, the P-CSCF discovers charging function addresses by other means not specified in this document.

- 3) shall remove the P-Access-Network-Info header field, if the request or the response include a P-Access-Network-Info header field with a "network-provided" parameter;
- 4) may insert a P-Access-Network-Info header field where:
  - a) if no mechanism exists to support the access technology for this UE, the "network-provided" parameter is included, and the access-type field is set to a preconfigured value;
  - b) if NASS is used to support the access technology for this UE, the "network-provided" parameter is included, and the access-type field is set:
    - when xDSL is the IP-CAN, to one of "ADSL", "ADSL2", "ADSL2+", "RADSL", "SDSL", "HDSL", "HDSL2", "G.SHDSL", "VDSL", or "IDSL", and the "dsl-location" parameter is set with the value received in the Location-Information header field in the User-Data Answer command as specified in ETSI ES 283 035 [98];
    - when Ethernet is the IP-CAN, to one of "IEEE-802.3", "IEEE-802.3a", "IEEE-802.3e", "IEEE-802.3i", "IEEE-802.3j", "IEEE-802.3u", "IEEE-802.3ab" or "IEEE-802.3ae", "IEEE-802.3ak", "IEEE-802.3aq", "IEEE-802.3an", "IEEE-802.3y" or "IEEE-802.3z" and if NASS subsystem is used, and the "eth-location" parameter is set with the value received in the Location-Information header field in the User-Data Answer command as specified in ETSI ES 283 035 [98];
    - when Fiber is the IP-CAN, to one of "G-PON", "XGPON1" or "IEEE-802.3ah" and if NASS subsystem is used, and the "fiber-location" parameter is set with the value received in the Location-Information header field in the User-Data Answer command as specified in ETSI ES 283 035 [98];
  - c) if the PCRF is used to support the access technology for this UE and 3GPP-User-Location-Info as specified in 3GPP TS 29.214 [13D] is not available:
    - if the IP-CAN-Type value provided by the PCRF is not "DVB-RCS2", then:
      - I) the access type field or the access-class field is set to a value consistent with that received from the PCRF in the IP-CAN-Type and RAT-Type parameters using the procedures specified in 3GPP TS 29.214 [13D];
      - II) if a 3GPP-MS-TimeZone parameter is available from the PCRF, then the local-time-zone field may also be added using this information; and
      - III) the "network-provided" parameter is added; and
    - if the IP-CAN-Type value provided by the PCRF is "DVB-RCS2", then the "network-provided" parameter is included, the access type field is set to "DVB-RCS2", and the "dvb-rcs2-node-id" parameter is set with the value provided by the IP-CAN provider;
  - d) if the PCRF is used to support the access technology for this UE and 3GPP-User-Location-Info as specified in 3GPP TS 29.214 [13D] is available:
    - I) the access-type field or the access-class field is set to a value consistent with that received from the PCRF in the IP-CAN-Type and RAT-Type parameters;

- II) the access-info field is set to a value consistent with the information received from the PCRF in the 3GPP-User-Location-Info parameter;
  - III) if a 3GPP-MS-TimeZone parameter is available from the PCRF, then the local-time-zone field may also be added using this information;
  - IV) the "network-provided" parameter is added; and
  - V) if required by local operator policy and the P-CSCF is able to deduce a Geographical Identifier from the Cell Global Identity (CGI) or from the Service Area Identifier (SAI) received from the PCRF, the P-CSCF shall include an operator-specific-GI field; and
- e) if DOCSIS is used, and proprietary means of obtaining a location are used, the access-type field is set to "DOCSIS" and the "network-provided" parameter is added; and
- 5) shall remove all Feature-Caps header fields, if present, from a UE that is not considered as privileged sender.

When the P-CSCF receives any request or response containing the P-Media-Authorization header field, the P-CSCF shall remove the header field.

NOTE 5: Depending on the security mechanism in use, the P-CSCF can integrity protect all SIP messages sent to the UE outside of the registration and authentication procedures by using a security association or TLS session. The P-CSCF will discard any SIP message that is not protected by using a security association or TLS session and is received outside of the registration and authentication procedures. The integrity and confidentiality protection and checking requirements on the P-CSCF within the registration and authentication procedures are defined in subclause 5.2.2.

With the exception of 305 (Use Proxy) responses, the P-CSCF shall not recurse on 3xx responses.

NOTE 6: If the P-CSCF is connected to a PDF the requirements for this interconnection is specified in the Release 6 version of this specification.

The P-CSCF may add, remove, or modify, the P-Early-Media header field within forwarded SIP requests and responses according to procedures in RFC 5009 [109].

NOTE 7: The P-CSCF can use the P-Early-Media header field for the gate control procedures, as described in 3GPP TS 29.214 [13D]. In the presence of early media for multiple dialogs due to forking, if the P-CSCF is able to identify the media associated with a dialog, (i.e., if symmetric RTP is used by the UE and the P-CSCF can use the remote SDP information to determine the source of the media) the P-CSCF can selectively open the gate corresponding to an authorized early media flow for the selected media.

When SIP digest without TLS is used, the P-CSCF shall discard any SIP messages received outside of the registration and authentication procedures that do not map to an existing IP association as defined in subclause 5.2.3.

In case a device performing address and/or port number conversions is provided by a NA(P)T or NA(P)T-PT controlled by the P-CSCF, the P-CSCF may need to modify the SIP contents according to the procedures described in annex F. In case a device performing address and/or port number conversions is provided by a NA(P)T or NA(P)T-PT not controlled by the P-CSCF, the P-CSCF may need to modify the SIP contents according to the procedures described in annex K if both a "reg-id" and "+sip.instance" header field parameters are present in the received Contact header field as described in RFC 5626 [92].

The P-CSCF shall support the provision of the user-related policies (e.g. consideration of the user as a privileged sender):

- from the S-CSCF during registration; and
- by local configuration.

For the same policy, the precedence between the locally configured policy and a policy received during registration shall be based on local operator policy.



## 5.2.2 Registration

### 5.2.2.1 General

The P-CSCF shall be prepared to receive the unprotected REGISTER requests on the SIP default port values as specified in RFC 3261 [26]. The P-CSCF shall also be prepared to receive the unprotected REGISTER requests on the port advertised to the UE during the P-CSCF discovery procedure.

NOTE 1: The P-CSCF will only accept further registration and subsequent SIP messages on the same ports for security mechanisms that do not require to use negotiated ports for exchanging protected messages.

The P-CSCF shall distinguish between security mechanisms through the use of the Security-Client header field and Authorization header field as follows:

- 1) if a REGISTER request from the UE contains a Security-Client header field and the Require and Proxy-Require header fields contain "sec-agree", then for an initial registration, the P-CSCF shall select the sec-mechanism and mode (as described in Annex H of 3GPP TS 33.203 [19]) from the corresponding parameters offered in the Security-Client header field according to its priorities, as follows:
  - if the P-CSCF selects the sec-mechanism "ipsec-3gpp" then follow the procedures as described in subclause 5.2.2.2, in addition to the procedures described in this subclause;
  - if the P-CSCF selects the sec-mechanism "tls" then follow the procedures as described in subclause 5.2.2.4, in addition to the procedures described in this subclause.

NOTE 2: If the Security-Client header field contains only media plane security mechanisms then Require and Proxy-Require header fields will not contain "sec-agree". The P-CSCF will then continue as per the procedure in bullet 2), not select a signalling plane security mechanism and then distinguish signalling plane security based upon the Authorization header field as described in the steps below.

2) if:

- a) a REGISTER request from the UE does not contain a Security-Client header field;
- b) a REGISTER request from the UE contains a Security-Client header field containing only media plane security mechanisms and the Require and Proxy-Require header fields do not contain "sec-agree"; or
- c) the P-CSCF does not select any signalling plane security mechanism from the Security-Client header field;

then the P-CSCF shall behave as follows, in addition to the procedures described in the remainder of this subclause:

- if the REGISTER request does not contain an Authorization header field and was received over an access network defined in 3GPP specifications then follow the GPRS-IMS-Bundled authentication procedures as described in subclause 5.2.2.6; or
- if the REGISTER request does not contain an Authorization header field and was received over a TISPN NASS and the P-CSCF supports both SIP digest and NASS-IMS bundled authentication, then the P-CSCF shall perform the steps required for NASS-IMS bundled authentication, in subclause 5.2.2.5, as well as the steps required for SIP digest without TLS, in subclause 5.2.2.3, unless it is configured to behave differently or the P-CSCF only supports either SIP digest without TLS or NASS-IMS bundled authentication. If the NASS-IMS bundled authentication related query from the P-CSCF to the TISPN NASS fails, then the P-CSCF shall only continue with the SIP digest related steps; or
- if the REGISTER request does not contain an Authorization header field, and was received over an access other than defined in 3GPP specifications or TISPN NASS, then follow the SIP digest without TLS procedures described in subclause 5.2.2.3; or

NOTE 3: How the P-CSCF recognizes over which access network a request was received is an implementation specific feature.

- if the REGISTER request contains an Authorization header field and was not received over a TISPN NASS then follow the SIP digest without TLS procedures as described in subclause 5.2.2.3; or

- if the REGISTER request contains an Authorization header field and was received over a TISpan NASS, and the P-CSCF supports both SIP digest and NASS-IMS bundled authentication, then the P-CSCF shall perform the steps required for NASS-IMS bundled authentication, in subclause 5.2.2.5, as well as the steps required for SIP digest without TLS, in subclause 5.2.2.3, unless it is configured to behave differently. If the NASS-IMS bundled authentication related query from the P-CSCF to the TISpan NASS fails, then the P-CSCF shall only continue with the SIP digest related steps.

For subsequent registrations, the P-CSCF shall continue to use the selected mechanism.

NOTE 4: The steps required for SIP digest and for NASS-IMS bundled authentication are not in contradiction. Rather, for NASS-IMS bundled authentication the P-CSCF needs to perform additional steps, namely an exchange with the TISpan NASS and an inclusion of NASS location information in the REGISTER request, on top of the steps required for SIP digest.

NOTE 5: How the P-CSCF knows the access network type of a specific network interface is implementation-dependent (e.g. it can know the access network type from different UE IP address ranges or by using different network interfaces for different access network types).

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

- 1) insert a Path header field in the request including an entry containing:
  - the SIP URI identifying the P-CSCF;
  - an indication that requests routed in this direction of the path (i.e. from the S-CSCF towards the P-CSCF) are expected to be treated as for the UE-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;
  - an IMS flow token in the user portion of the P-CSCF's SIP URI inserted into the Path header field, and the "ob" SIP URI parameter according to RFC 5626 [92]. The same SIP URI (user portion, hostport parameter and SIP URI parameters) shall be used for the initial registration, and the re-registrations, binding fetchings, and de-registration that refreshes of the respective registration;
  - the P-CSCF shall use a different IMS flow token for each registration. If the multiple registration mechanism is used, the P-CSCF shall also use a different IMS flow token for each registration flow associated with the registration;

NOTE 6: The form of the IMS flow token is of local significance to the P-CSCF only and can thus be chosen freely by a P-CSCF implementation.

NOTE 7: By inserting the "ob" SIP URI parameter in its SIP URI, the P-CSCF indicates that it supports multiple registrations as specified in RFC 5626 [92]. The presence of the "ob" SIP URI parameter is not an indication that the P-CSCF supports the keep-alive mechanism. When the P-CSCF detects that the UE is behind a NAT and the P-CSCF supports a keep-alive mechanism defined in RFC 5626 [92].

- 2) insert a Require header field containing the option-tag "path";
- 3) insert a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17] and a type 1 "orig-ioi" header field parameter. The P-CSCF shall set the type 1 "orig-ioi" header field parameter to a value that identifies the sending network of the request. The P-CSCF shall not include the type 1 "term-ioi" header field parameter;
- 4) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network;
- 4A) store the announcement of the media plane security mechanisms the UE supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Client header field, if any. Also, if the Security-Client header field contains only media plane security mechanisms, remove the header field;

NOTE 8: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

- 4B) if the REGISTER request contains an Authorization header field, remove the "integrity-protected" header field parameter, if present;

- 4C) if the host portion of the sent-by field in the topmost Via header field contains a FQDN, or if it contains an IP address that differs from the source address of the IP packet, the P-CSCF shall add a "received" Via header field parameter in accordance with the procedure defined in RFC 3261 [26];
- 5) if the P-CSCF is located in the visited network, and local policy requires the application of IBCF capabilities in the visited network towards the home network:

- a) if the request is not to be forwarded to an ATCF according to local policy select an exit point in visited network;

NOTE 9: The list of the exit points can be either obtained as specified in RFC 3263 [27A] or provisioned in the P-CSCF.

- b) if the request is to be forwarded to an ATCF according to local policy:
- i) insert a Route header field with the ATCF URI for originating requests; and
- ii) forward the request; and
- c) if the request is not to be forwarded to an ATCF according to local policy, then forward the request to the selected exit point.

If:

- no response is received to the REGISTER request and its retransmissions by the P-CSCF; or
- a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request;

the P-CSCF shall repeat the actions of this bullet with a different exit point or a different ATCF.

If the P-CSCF fails to forward the REGISTER request to any exit point or any ATCF, the P-CSCF shall send back a 504 (Server Time-Out) response to the user, in accordance with the procedures in RFC 3261 [26] unless local policy allows omitting the exit point;

NOTE 10: If the P-CSCF forwards the request to an IBCF in the visited network, the IBCF in the visited network can determine the entry point of the home network, as specified in RFC 3263 [27A] or the entry point of the home network can be provisioned in the IBCF in the visited network.

- 6) if the P-CSCF is located in the visited network and local policy does not require the application of IBCF capabilities in the visited network towards the home network:
- a) if the request is not to be forwarded to an ATCF according to local policy select an entry point of the home network;

NOTE 11: The list of the entry points can be either obtained as specified in RFC 3263 [27A] or provisioned in the P-CSCF.

- b) if the request is to be forwarded to an ATCF according to local policy:
- i) insert a Route header field with the ATCF URI for originating requests; and
- ii) forward the request; and
- c) if the request is not to be forwarded to an ATCF according to local policy, then forward the request to the selected entry point.

If:

- no response is received to the REGISTER request and its retransmissions by the P-CSCF; or
- a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request is received;

the P-CSCF shall repeat the actions of this bullet with a different entry point or a different ATCF.

If the P-CSCF fails to forward the REGISTER request to any entry point or any ATCF, the P-CSCF shall send back a 504 (Server Time-Out) response to the user, in accordance with the procedures in RFC 3261 [26]; and

- 7) if the P-CSCF is located in the home network:
- a) if the request is not to be forwarded to an ATCF according to local policy select the I-CSCF of the home network;

NOTE 12: The list of the I-CSCFs can be either obtained as specified in RFC 3263 [27A] or provisioned in the P-CSCF.

- b) if the request is to be forwarded to an ATCF according to local policy:
  - i) insert a Route header field with the ATCF URI for originating requests; and
  - ii) forward the request; and
- c) if the request is not to be forwarded to an ATCF according to local policy, then forward the request to the selected I-CSCF.

If:

- no response is received to the REGISTER request and its retransmissions by the P-CSCF; or
- a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request is received;

the P-CSCF shall repeat the actions of this bullet with a different I-CSCF or a different ATCF.

If the P-CSCF fails to forward the REGISTER request to any I-CSCF or any ATCF, the P-CSCF shall send back a 504 (Server Time-Out) response to the user, in accordance with the procedures in RFC 3261 [26].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the registration expiration interval value. When the registration expiration interval value is different than zero, then the P-CSCF shall:

- 1) save the list of service route values in the Service-Route header fields preserving the order, and bind the list either to the contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used) and the associated security association or TLS session over which the REGISTER request was received. The P-CSCF shall store this list during the entire registration period of the respective public user identity and bind it either to the associated contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used). The P-CSCF shall use this list to validate the routing information in the requests originated by the UE using either the respective contact address or to the registration flow and the associated contact address, and received over the respective security association or a TLS session. If the list of Service-Route header fields already exists either for this contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), then the P-CSCF shall replace the already existing list of service route values with the list of Service-Route header fields received in the 200 (OK) response;

NOTE 13: When the UE registers multiple registration flows and the associated contact addresses, then the UE and the P-CSCF will have a list of Service-Route header fields for each registration flow and the associated contact address and the associated security association or TLS session. When sending a request using a given registration flow and the associated contact address and the associated security association or TLS session, the UE will use the corresponding list of Service-Route header fields, when building a list of Route header fields.

- 2) associate the list of service route values with the registered public user identity and either the associated contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used) and the associated security association or TLS session;
- 3) store the public user identities, found in the P-Associated-URI header field value, including any associated display names, and any parameters associated with either the user or the identities of the user, and associate them to the registered public user identity, i.e. the registered public user identity and its associated set of implicitly registered public user identities are bound to the contact address and security association or TLS session over which the REGISTER request was received;
- 3A) if the user-related policies statically provisioned to the P-CSCF (see subclause 5.2.1) indicate that the URIs contained in the P-Associated-URI header field shall not be forwarded towards the UE, and the the P-CSCF is

located in the home operator network of the UE, then the P-CSCF shall remove all but the first URI contained in the P-Associated-URI header field of the 200 (OK) response;

NOTE 14: The URIs in the P-Associated-URI header field might need to be removed in case of the UE performs the functions of an external attached network (e.g an enterprise network).

- 4) store the default public user identity, including its associated display name, if provided, for use with procedures for the P-Asserted-Identity header field for requests received from the UE over the respective security association or TLS session. The default public user identity is the first on the list of URIs present in the P-Associated-URI header field;

NOTE 15: There can be more than one default public user identity stored in the P-CSCF, as the result of the multiple registrations of public user identities.

NOTE 16: For each contact address and the associated security association or TLS session the P-CSCF will maintain a list of registered public user identities and the associated default public user identities, that it will use when populating the P-Asserted Identity header.

- 5) store the values received in the P-Charging-Function-Addresses header field;
- 6) if a "term-ioi" header field parameter is received in the P-Charging-Vector header field, store the value of the received "term-ioi" header field parameter;

NOTE 17: Any received "term-ioi" header field parameter will contain a type 1 IOI. The type 1 IOI identifies the home network of the registered user.

- 7) if the P-CSCF included an IMS flow token and the "ob" SIP URI parameter in the Path header field of the REGISTER request, check for presence of the option-tag "outbound" in the Require header field of the a 200 (OK) response:
  - if the option-tag "outbound" is present, it indicates that the UE has successfully registered its public user identity with a new bidirectional flow as defined in RFC 5626 [92]. In this case the P-CSCF shall route the subsequent requests and responses destined for the UE as specified in RFC 5626 [92]; or
  - if the option-tag "outbound" is not present, it indicates that the public user identity has not been registered as specified in RFC 5626 [92]. In this case the P-CSCF shall route the subsequent requests and responses destined for the UE as specified in RFC 3261 [26]; and
- 8) if the P-CSCF detects that the UE is behind a NAT, and the UE's Via header field contains a "keep" header field parameter, the P-CSCF shall add a value to the parameter, to indicate that it is willing to receive keep-alives associated with the registration from the UE, as defined in RFC 6223 [143].

If the P-CSCF detects that the UE is behind a NAT, and the request was received over a TCP connection, the P-CSCF shall not close the TCP connection during the duration of the registration.

NOTE 18: The P-CSCF can conclude whether the UE is behind a NAT or not by comparing the values in the "received" header field parameter and "rport" header field parameter with the corresponding values in the sent-by parameter in the topmost Via header field. If the values do not match, the P-CSCF can conclude that the UE is behind a NAT.

### 5.2.2.2 IMS AKA as a security mechanism

When the P-CSCF receives a REGISTER request from the UE, as defined in subclause 5.2.2.1, the P-CSCF shall additionally:

- 1) insert the "integrity-protected" header field parameter (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received protected with the security association created during an ongoing authentication procedure and includes an authentication challenge response (i.e. RES parameter), or it was received on the security association created during the last successful authentication procedure, otherwise insert the parameter with the value "no";
- 1A) if the "reg-id" header field parameter was included in the Contact header field of the REGISTER request, insert in the Path header an IMS flow token and the "ob" URI parameter according to RFC 5626 [92]. The IMS flow token shall identify the flow from the P-CSCF toward the UE, as follows:

- a) for UDP, the IMS flow token identifies the unidirectional flow from the P-CSCF's protected client port and the P-CSCF's IP address to the UE's protected server port and the UE's IP address. This flow is used by the P-CSCF to send requests and responses to the UE. The P-CSCF shall receive the requests and responses from the UE on its protected server port; or
  - b) for TCP, the IMS flow token identifies the existing TCP connection between the UE and the P-CSCF. This TCP connection was established by the UE, i.e. from the UE's protected server port and the UE's IP address to the P-CSCF's protected client port and the P-CSCF's IP address. This TCP connection is used to exchange SIP messages between the UE and the P-CSCF;
- 2) in case the REGISTER request was received without protection, on the default port or port advertised to UE for P-CSCF discovery:
- a) check the existence of the Security-Client header field. If the Security-Client header field is present, then remove and store it. If the Security-Client header field is not present, then the P-CSCF shall return a suitable 4xx response;
  - b) set the value of the "rport" header field parameter in the Via header field to the source port of the received REGISTER request;
  - c) insert the "received" header field parameter in the Via header field containing the source IP address that the request came from, as defined in RFC 3581 [56A]; and

NOTE 1: As defined in RFC 3581 [56A], the P-CSCF will insert a "received" header field parameter containing the source IP address that the request came from, even if it is identical to the value of the "sent-by" component.

NOTE 2: Upon receiving the unprotected REGISTER request the P-CSCF detects if the UE is behind a NAT.

- 3) in case the REGISTER request was received protected, then towards the port that was notified to the UE in the previous response:
- a) check the security association which protected the request. If the security association is a temporary one, then the request is expected to contain a Security-Verify header field in addition to a Security-Client header field. If there are no such header fields, then the P-CSCF shall return a suitable 4xx response. If there are such header fields, then the P-CSCF shall compare the content of the Security-Verify header field with the content of the Security-Server header field sent earlier and the content of the Security-Client header field with the content of the Security-Client header field received in the challenged REGISTER request. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header field;
  - b) if the security association the REGISTER request was received on, is an already established one, then:
    - the P-CSCF shall remove the Security-Verify header field if it is present;
    - a Security-Client header field containing new parameter values is expected. If the Security-Client header field or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response; and
    - the P-CSCF shall remove and store the Security-Client header field before forwarding the request to the S-CSCF;
  - c) check if the private user identity conveyed in the Authorization header field of the protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response; and
  - d) ignore the "rport" Via header field parameter, if included.

NOTE 3: Once the IPsec security associations between the UE and the P-CSCF have been created, in case of UDP the P-CSCF sends the responses to a different UE's port than the one from which the request was received from the UE. For the TCP, the responses are sent on the TCP connection on which the request was received. Hence, the P-CSCF will ignore the "rport" Via header field parameter in all protected requests and responses, if received.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

- 1) delete any temporary set of security associations established towards the UE;
- 2) remove the "ck" and "ik" WWW-Authenticate header field parameters contained in the 401 (Unauthorized) response and bind the values to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the "ck" and "ik" header field parameters have been removed;
- 3) insert a Security-Server header field in the response, containing the P-CSCF static signalling plane security list and the parameters needed for this security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the IPsec layer algorithms for integrity and confidentiality protection as defined in 3GPP TS 33.203 [19] and shall announce support for them according to the procedures defined in RFC 3329 [48];
- 3A) insert a Security-Server header field to specify the media plane security mechanisms the P-CSCF (IMS-ALG) supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7;

NOTE 4 The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

- 4) set up the temporary set of security associations for this registration with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and
- 5) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected. If the 401 (Unauthorized) response to the unprotected REGISTER request is sent using UDP, the P-CSCF shall send the response to the IP address listed in the "received" Via header field parameter and the port in the "rport" Via header field parameter. In case of TCP, the P-CSCF shall send the response over the same TCP connection over which the request was received from the UE.

NOTE 5: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request as defined in subclause 5.2.2.1, the P-CSCF shall additionally:

- 1) if an existing set of security association is available, set the SIP level lifetime of the security association to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds;
- 2) if a temporary set of security associations exists, change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and
- 3) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the REGISTER request was protected.

If the P-CSCF receives a SIP message (including REGISTER requests) from the UE over the newly established set of security associations that have not yet been taken into use, the P-CSCF shall:

- 1) reduce the SIP level lifetime of the old set of security associations towards the same UE to  $64 \cdot T1$  (if currently longer than  $64 \cdot T1$ ); and
- 2) use the newly established set of security associations for further messages sent towards the UE as appropriate (i.e. take the newly established set of security associations into use).

NOTE 6: If the UE has registered other contact addresses and established security associations for these contact addresses, it can use them when sending subsequent SIP messages rather than using the newly established set of security associations. In this case the P-CSCF will not receive any SIP message over the newly established set of security associations.

NOTE 7: In this case, the P-CSCF will send requests (that specify the associated contact address in the Request-URI) towards the UE over the newly established set of security associations. Responses towards the UE that are sent via UDP will be sent over the newly established set of security associations. Responses towards the UE that are sent via TCP will be sent over the same set of security associations that the related request was received on.

NOTE 8: When receiving a SIP message (including REGISTER requests) from the UE over a set of security associations that is different from the newly established set of security associations, the P-CSCF will not take any action on any set of security associations.

When the SIP level lifetime of an old set of security associations is about to expire, i.e. their SIP level lifetime is shorter than  $64 * T1$  and a newly established set of security associations has not been taken into use, the P-CSCF shall use the newly established set of security associations for further messages towards the UE as appropriate (see NOTE 2).

When sending the 200 (OK) response for a REGISTER request that concludes a re-authentication, the P-CSCF shall:

- 1) keep the set of security associations that was used for the REGISTER request that initiated the re-authentication;
- 2) keep the newly established set of security associations created during this authentication; and
- 3) go on using for further requests sent towards the UE the set of security associations and associated contact address that was used to protect the REGISTER request that initiated the re-authentication as appropriate (see NOTE 6).

When sending the 200 (OK) response for a REGISTER request that concludes an initial authentication of the user registering its public user identity with a given contact address the associated security association, i.e. the REGISTER request that initiated the authentication was received unprotected, the P-CSCF shall:

- 1) keep the newly established set of security associations created during this authentication; and
- 2) use the kept newly established set of security associations and associated contact address for further messages sent towards the UE as appropriate (see NOTE 6).

NOTE 9: For each contact address or for each registration flow and the associated contact address and bound to a set of security associations the P-CSCF will maintain two Route header field lists. The first Route header field list (constructed from the Service-Route header fields received during the last registration procedure of either the respective contact address or a registration flow and the associated contact address) is used only to validate the routing information in the initial requests for a dialog and stand alone transactions originating from the UE using either the respective contact address or a registration flow and the associated contact address and are the respective security association. This list is valid as long as there is at least one public user identity registered either with the associated contact address or a registration flow and the associated contact address. The second list is the list of Route header fields (constructed from the Record Route header fields in the initial INVITE request and associated response) is used during the duration of the call. Once the call is terminated, this list of Route header fields is discarded.

The P-CSCF shall delete any security association from the IPsec database when their SIP level lifetime expires.

The handling of the security associations at the P-CSCF is summarized in table 5.2.2-1.



**Table 5.2.2-1: Handling of security associations at the P-CSCF**

|  | <b>Temporary set of security associations</b>  | <b>Newly established set of security associations</b>                      | <b>Old set of security associations</b>   |
|--|--|--|---|
| SIP message received over newly established set of security associations that have not yet been taken into use | No action  | Take into use  | Reduce SIP level lifetime to $64 \cdot T1$ , if lifetime is larger than $64 \cdot T1$   |
| SIP message received over old set of security associations   | No action  | No action  | No action   |
| Old set of security associations currently in use will expire in $64 \cdot T1$                                 | No action  | Take into use  | No action   |
| Sending an authorization challenge within a 401 (Unauthorized) response for a REGISTER request                 | Create<br>Remove any previously existing temporary set of security associations          | No action  | No action   |
| Sending 200 (OK) response for REGISTER request that concludes re-authentication                                | Change to a newly established set of security associations                               | Convert to and treat as old set of security associations (see next column) | Continue using the old set of security associations over which the REGISTER request, that initiated the re-authentication was received.<br>Delete all other old sets of security associations immediately |
| Sending 200 (OK) response for REGISTER request that concludes initial authentication                           | Change to a newly established set of security associations and take into use immediately | Convert to old set of security associations, i.e. delete                   | Delete  |

### 5.2.2.3 SIP digest without TLS as a security mechanism

When the P-CSCF receives a REGISTER request from the UE, as defined in subclause 5.2.2.1, the P-CSCF shall additionally:

- 1) if the REGISTER request includes an Authorization header field update the "integrity-protected" header field parameter as follows:
  - a) if the REGISTER request does not map to an existing IP association, and does not contain a challenge response, not include the "integrity-protected" header field parameter; or
  - b) if the REGISTER request does not map to an existing IP association, and does contain a challenge response, include an "integrity-protected" header field parameter with the value set to "ip-assoc-pending"; or
  - c) if the REGISTER request does map to an existing IP association, include an "integrity-protected" header field parameter with the value set to "ip-assoc-yes";

NOTE 1: The value of "ip-assoc-pending" for the "integrity-protected" header field parameter or the absence of an "integrity-protected" header field parameter in the Authorization header field is an indication to the I-CSCF and S-CSCF that this is an initial REGISTER request.

- 2) if the P-CSCF adds a "received" header field parameter and UDP is being used, also add an "rport" Via header field parameter with the IP source port of the received REGISTER request; and
- 3) if the REGISTER request does not contain an Authorization header field and the requests was received over a non 3GPP access network, insert a P-Access-Network-Info header field as described in subclause 5.2.1 step 4).

NOTE 2: How the P-CSCF recognizes over which access network a request was received is an implementation specific feature.

NOTE 3: Subclause 5.2.1 describes the encoding of the P-Access-Network-Info header field, the mandatory requirement is defined in the above bullet.

If the P-CSCF receives a 500 (Server Internal Error) or 504 (Server Time-Out) response to a REGISTER request, and if the REGISTER request is mapped to an existing IP association, then the P-CSCF shall delete the IP association.

NOTE 4: The P-CSCF deletes the IP association on receipt of 500 (Server Internal Error) or 504 (Server Time-Out) so that the next REGISTER request received from the UE will look like an initial REGISTER request.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

- 1) insert a Security-Server header field to specify the media plane security mechanisms the P-CSCF (IMS-ALG) supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7; and
- 2) send the 401 (Unauthorized) response to the UE unprotected as defined in clause 4 of RFC 3581 [56A].

NOTE 5: The P-CSCF does not include signalling plane security mechanisms because the Require and Proxy-Require header fields in the REGISTER request do not contain "sec-agree".

When the P-CSCF receives a 200 (OK) response to a REGISTER request as defined in subclause 5.2.2.1, and the registration expiration interval value is different than zero, the P-CSCF shall additionally:

- a) create an IP association by storing and associating the UE's packet source IP address and port along with the "sent-by" parameter of the Via header field, cf. RFC 3261 [26], of the REGISTER request with the private user identity and all the successfully registered public user identities related to that private user identity;
- b) overwrite any existing IP association which has the same pair of IP address and port, but a different private user identity; and
- c) send the 200 (OK) response to the UE unprotected as defined in clause 4 of RFC 3581 [56A].

#### 5.2.2.4 SIP digest with TLS as a security mechanism

TLS is optional to implement and is used only in combination with SIP digest authentication. If the P-CSCF supports TLS, then the P-CSCF shall support TLS as described in 3GPP TS 33.203 [19]. If the P-CSCF supports TLS, the P-CSCF shall support TLS ciphersuites as described in 3GPP TS 33.203 [19].

When the P-CSCF receives a REGISTER request from the UE, as defined in subclause 5.2.2.1, the P-CSCF shall additionally:

- 1) in case the REGISTER request was received without protection on the default port or port advertised to UE for P-CSCF discovery and with the Security-Client header field indicating "tls", then:
  - a) remove and store the Security-Client header field;
  - b) do not include the "integrity-protected" header field parameter in the Authorization header;
  - c) set the value of the "rport" header field parameter in the Via header to the source port of the received REGISTER request; and
  - d) insert the "received" header field parameter in the Via header containing the source IP address that the request came from, as defined in RFC 3581 [56A];

NOTE 1: The absence of an "integrity-protected" header field parameter in the Authorization header is an indication to the I-CSCF and S-CSCF that this is an initial REGISTER request.

NOTE 2: As defined in RFC 3581 [56A], the P-CSCF will insert a "received" header field parameter containing the source IP address that the request came from, even if it is identical to the value of the "sent-by" component.

NOTE 3: Upon receiving the unprotected REGISTER request the P-CSCF detects if the UE is behind a NAT.

- 2) if the REGISTER request was received protected with a TLS session, on the protected server port, created during an ongoing authentication procedure, where the Session ID for the TLS session is not yet bound to a private user identity, and contains an authentication challenge response (i.e. response parameter), then:
  - a) check if the private user identity conveyed in the Authorization header of the protected REGISTER request is the same as the private user identity which was previously challenged. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;

- b) check the existence of the Security-Verify header field and the Security-Client header field. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header field with the content of the Security-Server header field sent earlier and the content of the Security-Client header field with the content of the Security-Client header field received in the challenged REGISTER request. If those do not match, then there is a potential man-in-the-middle attack. The P-CSCF should reject the request by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header fields;
  - c) include an "integrity-protected" header field parameter with the value set to "tls-pending"; and
  - d) if the hostport parameter in the Contact header field is in the form of a FQDN, the P-CSCF shall ensure that the given FQDN will resolve (e.g. by reverse DNS lookup) to the IP address bound to the TLS session; or
- 2A) if the REGISTER request was received, protected with a TLS session on the protected server port, created during an ongoing authentication procedure, where the Session ID for the TLS session is not yet bound to a private user identity, and does not contain an authentication challenge response (i.e. response parameter), reject the REGISTER request by returning a 403 (Forbidden) response;
- 3) if the REGISTER request was received on an existing TLS session created during a previous authentication procedure, then:
- a) if the REGISTER request includes an Authorization header field, check if the private user identity conveyed in the Authorization header of the protected REGISTER request is the same as the private user identity which was previously authenticated, i.e. the private user identity previously associated with the Session ID for this TLS session. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;
  - b) check the existence of the Security-Verify header field and Security-Client header field. If there are no such header fields, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header field with the content of the Security-Server header field sent earlier and the content of the Security-Client header field with the content of the Security-Client header field received in the challenged REGISTER request. If those do not match, then there is a potential man-in-the-middle attack. The P-CSCF should reject the request by sending a suitable 4xx response;
  - c) the P-CSCF shall remove and store the Security-Client header field and remove the Security-Verify header field before forwarding the request to the S-CSCF; and
  - d) include an "integrity-protected" header field parameter with the value set to "tls-yes".

If the P-CSCF require security agreement, and the Security-Client header field is not present, then the P-CSCF shall return a suitable 4xx response.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

- 1) insert a Security-Server header field in the response, containing the P-CSCF selected signalling plane mechanism name, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support and indicate the "tls" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the TLS ciphersuites as described in 3GPP TS 33.203 [19] and shall announce support for them according to the procedures defined in RFC 3329 [48]; and
- 1A) insert a Security-Server header field in the response, containing the P-CSCF static media plane security list, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7;
- 2) send the 401 (Unauthorized) response to the UE using the TLS session with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected. If the 401 (Unauthorized) response to the unprotected REGISTER request is sent using UDP, the P-CSCF shall send the response to the IP address listed in the "received" header field parameter and the port in the "rport" header field parameter. In case of TCP, the P-CSCF shall send the response over the same TCP connection over which the request was received from the UE.

NOTE 4: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it.

When the P-CSCF receives a 200 (OK) response to a REGISTER request as defined in subclause 5.2.2.1, and the registration expiration interval value is different than zero, the P-CSCF shall additionally:

- create an association by storing and associating the UEs IP address and port of the TLS connection with the TLS Session ID, the private user identity and all the successfully registered public user identities related to that private user identity; and
- protect the 200 (OK) response to the REGISTER request within the same TLS session to that in which the request was protected.

#### 5.2.2.5 NASS-IMS bundled authentication as a security mechanism

When the P-CSCF receives a REGISTER request from the UE, as defined in subclause 5.2.2.1, the P-CSCF shall additionally:

- 1) perform the NASS-IMS bundled authentication related query from the P-CSCF to the TISpan NASS;
- 2) if the query in step 1) is successful, insert a P-Access-Network-Info header field as described in subclause 5.2.1 step 4); and
- 3) if the P-CSCF adds a "received" header field parameter and UDP is being used, the P-CSCF shall also add an "rport" Via header field parameter with the IP source port of the received REGISTER request.

When the P-CSCF receives a 200 (OK) response to a REGISTER request from the UE, as defined in subclause 5.2.2.1, the P-CSCF shall additionally:

- 1) store an association between the IP source address and port of the initial REGISTER request and the public user identities found in the P-Associated-URI header field value and associate them to the public user identity under registration;
- 2) store an association between the IP source address and port of the initial REGISTER request the default public user identity for use with procedures for the P-Asserted-Identity header field. The default public user identity is the first on the list of URIs present in the P-Associated-URI header field; and
- 3) insert a Security-Server header field to specify the media plane security mechanisms the P-CSCF (IMS-ALG) supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7.

NOTE 3: The P-CSCF does not include signalling plane security mechanisms because the Require and Proxy-Require header fields in the REGISTER request do not contain "sec-agree".

#### 5.2.2.6 GPRS-IMS-Bundled authentication as a security mechanism

When the P-CSCF receives a SIP request from a GPRS-IMS-Bundled UE, the P-CSCF checks the IP address in the "sent-by" parameter of the Via header field provided by the UE as specified in RFC 3261 [6]. If the "sent-by" parameter contains a domain name, or if it contains an IP address that differs from the packet source IP address, the P-CSCF adds a "received" header field parameter to that Via header field value. This parameter contains the source IP address from which the packet was received.

When the P-CSCF receives a 200 (OK) response to a REGISTER request from the UE, as defined in subclause 5.2.2.1, the P-CSCF shall additionally:

- 1) store an association between the IP source address and port of the initial REGISTER request and the public user identities found in the P-Associated-URI header field value and associate them to the public user identity under registration;
- 2) store an association between the IP source address and port of the initial REGISTER request the default public user identity for use with procedures for the P-Asserted-Identity header field. The default public user identity is the first on the list of URIs present in the P-Associated-URI header field;
- 3) if the P-CSCF adds a "received" header field parameter and UDP is being used, the P-CSCF shall also add an "rport" Via header field parameter with the IP source port of the received REGISTER request; and
- 4) insert a Security-Server header field to specify the media plane security mechanisms the P-CSCF (IMS-ALG) supports, if any, labelled with the "mediasec" header field parameter specified in subclause 7.2A.7.

NOTE: The P-CSCF does not include signalling plane security mechanisms because the Require and Proxy-Require header fields in the REGISTER request do not contain "sec-agree".

### 5.2.2.7 P-CSCF reconfigured to not accept registrations

If the P-CSCF has been reconfigured to not accept initial registrations and reregistrations and to redirect incoming registrations to another P-CSCF, on reception of a REGISTER request the P-CSCF shall return a 305 (Use Proxy) response.

NOTE 1: As an example, this situation can happen in case the P-CSCF has been administratively configured to force the UEs to attempt initial registration with another P-CSCF before shutdown.

NOTE 2: The UE does not use the Contact header field of 305 (Use Proxy) response to determine the IP address of the new P-CSCF through which the UE will attempt a new initial registration.

## 5.2.3 Subscription to the user's registration-state event package

Upon receipt of a 200 (OK) response to the first initial REGISTER request (i.e. this was the first initial REGISTER request that the P-CSCF received from the user identified with its private user identity), the P-CSCF shall:

- 1) generate a SUBSCRIBE request in accordance with RFC 3680 [43], with the following elements:
  - a Request-URI set to the resource to which the P-CSCF wants to be subscribed to, i.e. to the SIP URI that is the default public user identity of the user;
  - a From header field set to the P-CSCF's SIP URI;
  - a To header field, set to the SIP URI that is the default public user identity of the user;
  - an Event header field set to the "reg" event package;
  - an Expires header field set to a value higher than the registration expiration interval value indicated in the 200 (OK) response to the REGISTER request;
  - a P-Asserted-Identity header field set to the SIP URI of the P-CSCF, which was inserted into the Path header field during the registration of the user to whose registration state the P-CSCF subscribes to; and
  - a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17];
- 2) if the P-CSCF is located in the visited network, and local policy requires the application of IBCF capabilities in the visited network towards the home network, then the P-CSCF shall forward the request to an IBCF in the visited network;
- 3) if the P-CSCF is located in the visited network and local policy does not require the application of IBCF capabilities in the visited network towards the home network, determine the entry point of the home network (e.g., by using DNS services) and send the SUBSCRIBE request to that entry point, according to the procedures of RFC 3261 [26]; and
- 4) if the P-CSCF is located in the home network, then the P-CSCF shall forward the request to an I-CSCF in the home network.

NOTE: The subscription to reg event package is done once per private user identity.

Upon receipt of a 2xx response to the SUBSCRIBE request, the P-CSCF shall store the information for the so established dialog and the expiration time as indicated in the Expires header field of the received response.

If continued subscription is required the P-CSCF shall automatically refresh the subscription by the reg event package 600 seconds before the expiration time for a previously registered public user identity, either 600 seconds before the expiration time if the initial subscription was for greater than 1200 seconds, or when half of the time has expired if the initial subscription was for 1200 seconds or less. If a SUBSCRIBE request to refresh a subscription fails with a non-481 response, the P-CSCF shall still consider the original subscription valid for the duration of the most recently known "Expires" value according to RFC 3265 [28]. Otherwise, the P-CSCF shall consider the subscription invalid and start a new initial subscription according to RFC 3265 [28].

## 5.2.3A Void

### 5.2.3B SUBSCRIBE request

Upon receipt of a NOTIFY request with the Subscription-State header field set to "terminated", once the NOTIFY transaction is terminated, the P-CSCF can remove all the stored information related to the associated subscription.

## 5.2.4 Registration of multiple public user identities

Upon receipt of a 2xx response to the SUBSCRIBE request the P-CSCF shall maintain the generated dialog (identified by the values of the Call-ID header field, and the values of tags in To and From header fields).

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package of the user, the P-CSCF shall identify the public user identity as follows:

- 1) if no <wildcardedIdentity> subelement is included in the <registration> element, the public user identity is taken from the 'aor' attribute of the registration element; or
- 2) if a <wildcardedIdentity> sub element is included in the <registration> element, the wildcarded public user identity is taken from the <wildcardedIdentity> sub element. The wildcarded public user identity is treated as a public user identity in the procedures of this subclause.

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package of the user, the P-CSCF shall perform the following actions:

- 1) for each public user identity whose state attribute in the <registration> element is set to "active", i.e. registered; and
  - the state attribute within the <contact> sub-element is set to "active"; and
  - the value of the <uri> sub-element inside the <contact> sub-element is set to the contact address of the user's UE; and
  - the event attribute of that <contact> sub-element(s) is set to "registered" or "created";

the P-CSCF shall:

- bind the indicated public user identity as registered to the contact address of the respective user, including any associated display names, and any parameters associated with either the user or the identities of the user;
  - add the public user identity to the list of the public user identities that are registered for the user saved against the contact address;
  - if the <actions> child element is included in the <registration> element, bind the policy received in the <actions> child element of the <registration> element to each contact address of the public user identity; and
  - if the <actions> child element is not included in the <registration> element, remove the policy bound to each contact address of the public user identity;
- 2) for each public user identity whose state attribute in the <registration> element is set to "active", i.e. registered; and
    - the state attribute within the <contact> sub-element is set to "terminated";
    - the value of the <uri> sub-element inside the <contact> sub-element is set to the contact address of the user's UE; and
    - the event attribute of that <contact> sub-element(s) is set to "deactivated", "expired", "probation", "unregistered", or "rejected";

the P-CSCF shall consider the binding between the indicated public user identity and the contact address and its related information as deregistered for this user, and shall release all stored information associated with the deregistered contact address and related information associated with this contact address; and

- 3) for each public user identity whose state attribute in the <registration> element is set to "terminated", i.e. deregistered; and for each <contact> sub-element, if
- the value of the <uri> sub-element inside each <contact> sub-element is set to the respective contact address of the user's UE; and
  - the event attribute of each <contact> sub-element(s) is set to "deactivated", "expired", "probation", "unregistered", or "rejected";

the P-CSCF shall consider the indicated public user identity and all its contact addresses as deregistered for this UE, and shall release all stored information for these public user identity bound to the respective user and remove the public user identity from the list of the public user identities that are registered for the user.

If the P-CSCF is informed that all contact addresses that are registered with this P-CSCF and belonging to the user using its private user identity have been deregistered, i.e. the state attribute within each <contact> sub-element is set to "terminated", the P-CSCF shall either unsubscribe to the reg event package or let the subscription expire.

NOTE 1: Since there can be other active registrations of the user via other P-CSCFs, the S-CSCF will not terminate the by sending a NOTIFY request that includes the Subscription-State header set to "terminated".

If all public user identities, that were registered by the user using its private user identity, have been deregistered, the P-CSCF, will receive from the S-CSCF a NOTIFY request that may include the Subscription-State header field set to "terminated", as described in subclause 5.4.2.1.2. If the Subscription-State header field was not set to "terminated", the P-CSCF may either unsubscribe to the reg event package of the user or let the subscription expire.

NOTE 2: Upon receipt of a NOTIFY request with the Subscription-State header field set to "terminated", the P-CSCF considers the subscription to the reg event package terminated (i.e. as if the P-CSCF had sent a SUBSCRIBE request with an Expires header field containing a value of zero).

NOTE 3: There can be public user identities which are implicitly registered within the registrar (S-CSCF) of the user upon registration of one public user identity. The procedures in this subclause provide a mechanism to inform the P-CSCF about these implicitly registered public user identities.

## 5.2.5 Deregistration

### 5.2.5.1 User-initiated deregistration

When the P-CSCF receives a 200 (OK) response to a REGISTER request (sent according to subclause 5.2.2) sent by this UE, then the P-CSCF shall check each Contact header field included in the response. If there is a Contact header field that contains the contact address registered via this P-CSCF via the respective security associations or TLS sessions, and the value of the registration expiration interval value equals zero, then the P-CSCF shall:

- 1) if the "reg-id" header field parameter is not included in the Contact header field, remove the binding between the public user identity found in the To header field (together with the implicitly registered public user identities) and the contact address indicated in the Contact header field, from the registered public user identities list belonging to this UE and all related stored information;
- 1A) if the "reg-id" header field parameter is included in the Contact header field, remove the public user identity found in the To header field (together with the implicitly registered public user identities) and the flow identified by the "reg-id" header field parameter and all its related stored information belonging to this UE;
- 2) if multiple registrations is not used, check if the UE has left any other registered public user identity. When all of the public user identities that were registered by this UE are deregistered, the P-CSCF shall delete any security associations, TLS sessions or IP associations towards the UE, after the server transaction (as defined in RFC 3261 [26]) pertaining to this deregistration terminates; and
- 2A) if multiple registrations is used, check if the UE has left any other registered public user identity that is bound to this flow. When all of the public user identities that were registered and are bound to this flow are deregistered, the P-CSCF shall delete any security associations or TLS sessions associated with this flow, after the server transaction (as defined in RFC 3261 [26]) pertaining to this deregistration terminates.

NOTE 1: Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header field set to "terminated", the P-CSCF considers the subscription to the reg event package terminated (i.e. as if the P-CSCF had sent a SUBSCRIBE request with an Expires header field containing a value of zero).

NOTE 2: There is no requirement to distinguish a REGISTER request relating to a registration from that relating to a deregistration. For administration reasons the P-CSCF may distinguish such requests, however this has no impact on the SIP procedures.

NOTE 3: When the P-CSCF has sent the 200 (OK) response for the REGISTER request of the only public user identity currently registered with its associated set of implicitly registered public user identities using the respective security association or TLS session (i.e. no other public user identity belonging to the user is registered with this contact address the associated security association or TLS session), the P-CSCF removes the security association or TLS session established between the P-CSCF and the UE. Therefore further SIP signalling sent over this security association or TLS session (e.g. the NOTIFY request containing the deregistration event) will not reach the UE.

### 5.2.5.2 Network-initiated deregistration

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package of the UE, as described in subclause 5.2.3, including one or more <registration> element(s) which were registered by the UE with either:

- the state attribute within the <registration> element set to "terminated"; or
- the state attribute within the <registration> element set to "active" and the state attribute within the <contact> sub-element belonging to this UE and registered via this P-CSCF set to "terminated", and the event attribute within the <contact> sub-element belonging to this UE set either to "unregistered", or "rejected" or "deactivated";

the P-CSCF shall remove all stored information for these public user identities for this UE and remove these public user identities from the list of the public user identities that are registered for the user.

NOTE 1: If all public user identities have been removed from the list of the public user identities registered via this P-CSCF, and the NOTIFY request indicates that the UE is still registered (e.g. via another P-CSCF), the P-CSCF can unsubscribe from the reg event package of the UE.

Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header field set to "terminated" or when all public user identities of the UE have been deregistered, the P-CSCF shall shorten any security associations or TLS sessions towards the UE.

NOTE 2: The security association between the P-CSCF and the UE is shortened to a value that will allow the NOTIFY request containing the deregistration event to reach the UE.

NOTE 3: When the P-CSCF receives the NOTIFY request with Subscription-State header field containing the value of "terminated", the P-CSCF considers the subscription to the reg event package terminated (i.e. as if the P-CSCF had sent a SUBSCRIBE request to the S-CSCF with an Expires header field containing a value of zero).

## 5.2.6 General treatment for all dialogs and standalone transactions excluding the REGISTER method

### 5.2.6.1 Introduction

The procedures of subclause 5.2.6 and its subclauses are general to all requests and responses, except those for the REGISTER method.

### 5.2.6.2 Determination of UE-originated or UE-terminated case

Upon receipt of an initial request or a target refresh request or a stand-alone transaction, the P-CSCF shall:

- perform the procedures for the UE-terminating case as described in subclause 5.2.6.4 if the request makes use of the information for UE-terminating calls, which was added to the Path header field entry of the P-CSCF during registration (see subclause 5.2.2), e.g. the message is received at a certain port or the topmost Route header field contains a specific user part or parameter;
- perform the procedures for the UE-originating case as described in subclause 5.2.6.3 if this information is not used by the request.



### 5.2.6.3 Requests initiated by the UE

#### 5.2.6.3.1 General for all requests

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction from a UE that is not considered as privileged sender, and:

- the request does not include any P-Preferred-Identity header field or none of the P-Preferred-Identity header fields included in the request matches any of the registered public user identities or any of the registered wildcarded public user identities, then the P-CSCF shall identify the originator and the served user of the request by the default public user identity;
- the request includes one or two P-Preferred-Identity header field(s) each of which matches one of the registered public user identity or a registered wildcarded public user identity, the P-CSCF shall identify the originator and the served user of the request by the public user identity from the first such P-Preferred-Identity header field; and
- the request includes two P-Preferred-Identity header fields, each of which matches a registered public user identity or a registered wildcarded public user identity, the P-CSCF shall identify the alternative identity of the originator of the request by the public user identity from the second such P-Preferred-Identity header field.

NOTE: When two identities are provided in the P-Preferred-Identity header fields, it is assumed that one is an alias of the other but P-CSCF does not have the information to verify this.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction from a UE that is considered as privileged sender, and the request:

- a) does not include any P-Preferred-Identity header field, then the P-CSCF shall identify the served user of the request by the default public user identity;
- b) includes a P-Preferred-Identity header field that does not match one of the registered public user identities or wildcarded public user identities, then the P-CSCF shall identify the served user of the request by the default public user identity; or
- c) includes a P-Preferred-Identity header field that matches one of the registered public user identities or wildcarded public user identities, then the P-CSCF shall identify the served user of the request by the public user identity from the P-Preferred-Identity header field.

In addition, if the request from a UE that is considered as privileged sender:

- 1) includes one or two P-Asserted-Identity header field(s) then the P-CSCF shall identify the originator of that request by the public user identity from the first P-Asserted-Identity header field; or
- 2) does not include a P-Asserted-Identity header field then the P-CSCF shall identify the originator of that request by the same identity that has been determined for the served user according to steps a), b), and c) above.

NOTE 1: If no security association was set-up during registration, the P-CSCF identifies the originator and served user of the request by using the IP association information stored during the registration for which it holds the list of registered public user identities.

NOTE 2: The contents of the From header field do not form any part of this decision process.

NOTE 3: The display-name portion of the P-Preferred-Identity header field and the registered public user identities is not included in the comparison to determine a match.

NOTE 4: The P-CSCF determines if the UE is considered as privileged sender using the user-related policies provisioned to the P-CSCF (see subclause 5.2.1).

When the P-CSCF receives from the UE an initial request for a dialog or a request for a standalone transaction, if the host portion of the sent-by field in the topmost Via header field contains a FQDN, or if it contains an IP address that differs from the source address of the IP packet, the P-CSCF shall add a "received" header field parameter in accordance with the procedure defined in RFC 3261 [26].

If the P-CSCF adds a "received" header field parameter and UDP is being used, the P-CSCF shall also add an "rport" header field parameter. If IMS AKA is used, the parameter value shall contain the UEs protected server port. Otherwise the parameter value shall contain the IP source of the request.

### 5.2.6.3.2 Void

#### 5.2.6.3.2A Abnormal cases

When the P-CSCF is unable to forward the request to the next hop by the Route header fields, as determined by one of the following:

- there is no response to the service request and its retransmissions by the P-CSCF; or
- by unspecified means available to the P-CSCF;

and:

- the P-CSCF supports S-CSCF restoration procedures;

then the P-CSCF:

- 1) shall reject the request by returning a 504 (Server Time-out) response to the UE;
- 2) shall assume that the UE supports version 1 of the XML Schema for the 3GPP IM CN subsystem XML body if support for the 3GPP IM CN subsystem XML body as described in subclause 7.6 in the Accept header field is not indicated; and
- 3) shall include in the 504 (Server Time-out) response:
  - a Content-Type header field with the value set to associated MIME type of the 3GPP IM CN subsystem XML body as described in subclause 7.6.1;
  - a P-Asserted-Identity header field set to the value of the SIP URI of the P-CSCF included in the Path header field during the registration of the user whose UE sent the request causing this response (see subclause 5.2.2.1); and
  - a 3GPP IM CN subsystem XML body containing:
    - a) an <ims-3gpp> element with the "version" attribute set to "1" and with an <alternative-service> child element, set to the parameters of the alternative service:
      - i) a <type> child element, set to "restoration" (see table 7.6.2) to indicate that S-CSCF restoration procedures are supported;
      - ii) a <reason> child element, set to an operator configurable reason; and
      - iii) an <action> child element, set to "initial-registration" (see table 7.6.3).

NOTE: These procedures do not prevent the usage of unspecified reliability or recovery techniques above and beyond those specified in this subclause.

If the P-CSCF receives a SIP request different from REGISTER that does not map to an existing IP association and unless the P-CSCF detects that the request is related to an emergency communication that is to be handled according to subclause 5.2.10.2, the P-CSCF shall discard this SIP request, i.e. it shall not send back a 100 Trying SIP response to the UE and shall not try to forward the request to the S-CSCF.

NOTE: Reception of SIP requests not corresponding to a stored registration context may happen if the P-CSCF has lost the registration context. If the UE does not receive any SIP response to the sent SIP request (i.e. the SIP transaction timer B or F expires), the UE will perform a new initial registration procedure.

#### 5.2.6.3.3 Initial request for a dialog

When the P-CSCF receives from the UE an initial request for a dialog, and a service route value list exists for the served user of the request, the P-CSCF shall:

- 1) remove its own SIP URI from the top of the list of Route header fields;
- 2) verify that the resulting list of Route header fields matches the list of URIs received in the Service-Route header field (during the last successful registration or re-registration). This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

- a) return a 400 (Bad Request) response; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or
  - b) replace the preloaded Route header field value in the request with the value of the Service-Route header field received during the last 200 (OK) response for the last successful registration or reregistration;
- 3) if the 200 (OK) response to the last REGISTER request, which created or refreshed the binding of the contact address from which the request is received, has not contained a Feature-Caps header field, specified in RFC 6809 [190] with a "+g.3gpp.atcf" header field parameter, then:
- a) if the P-CSCF is located in the visited network, and local policy requires the application of IBCF capabilities in the visited network towards the home network, select an IBCF in the visited network and add the URI of the selected IBCF to the topmost Route header field;

NOTE 1: It is implementation dependent as to how the P-CSCF obtains the address of the IBCF exit point.

- 3A) if the 200 (OK) response to the last REGISTER request, which created or refreshed the binding of the contact address from which the request is received, contained a Feature-Caps header field with a "+g.3gpp.atcf" header field parameter, then:
- a) add the ATCF URI for originating requests that the P-CSCF used to forward the last REGISTER request which created or refreshed the binding of the contact address from which the request is received, to the topmost Route header field;
- 4) add its own address to the Via header field. The P-CSCF Via header field entry is built in a format that contains the port number of the P-CSCF in accordance with the procedures of RFC 3261 [26], and either:
- a) the P-CSCF FQDN that resolves to the IP address, or
  - b) the P-CSCF IP address;
- 5) when adding its own SIP URI to the Record-Route header field, build the P-CSCF SIP URI in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:
- a) the P-CSCF FQDN that resolves to the IP address; or
  - b) the P-CSCF IP address.

If the Contact header field in the request contains an "ob" SIP URI parameter, the P-CSCF shall add a flow token and the "ob" SIP URI parameter to its SIP URI;

NOTE 2: The inclusion of these values in the Record-Route header field will ensure that all subsequent mid dialog requests destined for the UE are sent over the same IMS flow over which the initial dialog-forming request was received.

- 5A) if a P-Private-Network-Indication header field is included in the request, check whether the information saved during registration or from configuration allows the receipt of private network traffic from this source. If private network traffic is allowed, the P-CSCF shall check whether the received domain name in any included P-Private-Network-Indication header field in the request is the same as the domain name associated with that saved information. If private network traffic is not allowed, or the received domain name does not match, then the P-CSCF shall remove the P-Private-Network-Indication header field;
- 5B) if the served user of the request is understood from information saved during registration or from configuration to always send and receive private network traffic from this source, insert a P-Private-Network-Indication header field containing the domain name associated with that saved information;
- 5C) if the request is originated from a UE which the P-CSCF considers as privileged sender, keep the P-Asserted-Identity header field unchanged if one was received, or include the originator of the request in the P-Asserted-Identity header field if no P-Asserted-Identity header field was received. In addition remove any P-Preferred-Identity header field, include the served user of the request in the P-Served-User header field as specified in RFC 5502 [133] and skip step 6) below;

NOTE 3: The P-CSCF determines if the UE is considered as privileged sender using the user-related policies provisioned to the P-CSCF (see subclause 5.2.1).

- 6) remove any P-Preferred-Identity header field or P-Asserted-Identity header field, if present, and insert a P-Asserted-Identity header field with the value identifying the originator of the request and the value of the alternative identity of the originator of the request, if identified (see subclause 5.2.6.3.1), including the display name if previously stored during registration representing the served user of the request;
- 6A) if the identity of the served user of the request was taken from P-Preferred-Identity header field by matching a registered wildcarded public user identity, and the identity of the served user is not a distinct identity within the range of the wildcarded public user identity, include the wildcarded public user identity value in the P-Profile-Key header field as defined in RFC 5002 [97];

NOTE 4: The matching of distinct public user identities takes precedence over the matching of wildcarded public user identities.

- 7) add a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17]; and
- 8) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed. If the Contact header field in the INVITE request contains a GRUU but it does not include an "ob" SIP URI parameter as defined in RFC 5626 [92], the P-CSCF shall save the GRUU received in the Contact header field of the request and associate that GRUU with the UE IP address and the UE port such that the P-CSCF is able to release the session if needed. The UE port used for the association is determined as follows:
  - if IMS AKA or SIP digest with TLS is being used as a security mechanism, the UE protected server port for the security association on which the request was received; or
  - if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled Authentication is being used as a security mechanism, the UE unprotected port on which the request was received;

before forwarding the request, based on the topmost Route header field, in accordance with the procedures of RFC 3261 [26].

NOTE 5: According to RFC 5626 [92], an approach such as having the Edge Proxy add a Record-Route header field with a flow token is one way to ensure that mid-dialog requests are routed over the correct flow.

#### 5.2.6.3.4 Responses to an initial request for a dialog

When the P-CSCF receives any 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) store the values received in the P-Charging-Function-Addresses header field;
- 2) store the list of Record-Route header fields from the received response;
- 3) store the dialog ID and associate it with the private user identity and public user identity involved in the session;
- 4) if a security association or TLS session exists, in the response rewrite its own Record Route entry to its own SIP URI that contains the protected server port number of the security association or TLS session established from the UE to the P-CSCF and either:
  - a) the P-CSCF FQDN that resolves to the IP address of the security association or TLS session established from the UE to the P-CSCF; or
  - b) the P-CSCF IP address of the security association or TLS session established from the UE to the P-CSCF;

NOTE 1: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port values see 3GPP TS 33.203 [19].

- 5) if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is used, in the response rewrite its own Record-Route entry to its own SIP URI that contains an unprotected server port number where the P-CSCF expects subsequent requests from the UE; and
- 6) if the response corresponds to an INVITE request, save the Contact, From, To and Record-Route header field values received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

NOTE 2: The P-CSCF can find the IMS communication service supported for the dialog, as determined by the originating home network, in the topmost occurrence of the "+g.3gpp.icsi-ref" header field parameter of the Feature-Caps header field(s) of 1xx or 2xx response. The information can be used for charging purpose or resource reservation purpose.

#### 5.2.6.3.5 Target refresh request for a dialog

When the P-CSCF receives from the UE a target refresh request for a dialog, the P-CSCF shall:

- 1) verify if the request relates to a dialog in which the originator of the request is involved:
  - a) if the request does not relate to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The P-CSCF will not forward the request. No other actions are required; or
  - b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;
    - 1A) remove its own SIP URI from the top of the list of Route header fields;
- 2) verify that the resulting list of Route header fields matches the list of Record-Route header fields constructed by inverting the order of the stored list of Record-Route header fields and removing its Record-Route header field value from the list. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) return a 400 (Bad Request) response; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
  - b) replace the Route header field value in the request with the list of Record-Route header fields constructed by inverting the order of the stored list of Record-Route header fields and removing its Record-Route header value from the list;
- 3) add its own address to the Via header field. The P-CSCF Via header field entry is built in a format that contains the port number of the P-CSCF where it awaits the responses to come, and either:
  - a) the P-CSCF FQDN that resolves to the IP address, or
  - b) the P-CSCF IP address;
- 4) void
- 5) for INVITE dialogs (i.e. dialogs initiated by an INVITE request), replace the saved Contact and CSeq header field values received in the request such that the P-CSCF is able to release the session if needed. If the Contact header field in the INVITE request contains a GRUU but the Contact header field does not include an "ob" SIP URI parameter as defined in RFC 5626 [92], the P-CSCF shall save the GRUU received in the Contact header field of the request and associate that GRUU with the UE IP address and the UE port such that the P-CSCF is able to release the session if needed. The UE port used for the association is determined as follows:
  - if IMS AKA or SIP digest with TLS is being used as a security mechanism, the UE protected server port for the security association on which the request was received; or
  - if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled Authentication is being used as a security mechanism, the UE unprotected port on which the request was received; and

NOTE: The replaced Contact header field value is valid only if a 1xx or 2xx response will be received for the request. In other cases the old value is still valid.

- 6) if the P-CSCF inserted the header field parameters into the Feature-Caps header field of the initial request for the dialog then when the target refresh request is forwarded in the same direction, the P-CSCF shall insert the header field parameters with the same parameter values in the Feature-Caps header field;

before forwarding the request, based on the topmost Route header field, in accordance with the procedures of RFC 3261 [26].

### 5.2.6.3.6 Responses to a target refresh request for a dialog

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) if a security association or TLS session exists, rewrite the the address and port number of its own Record Route entry to the same value as for the response to the initial request for the dialog; and
- 2) replace the saved Contact header field value received in the response such that the P-CSCF is able to release the session if needed;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

### 5.2.6.3.7 Request for a standalone transaction

When the P-CSCF receives from the UE the request for a standalone transaction, and a service route value list exists for the served user of the request, the P-CSCF shall:

- 1) remove its own SIP URI from the top of the list of Route header fields;
- 2) verify that the resulting list of Route header fields matches the list of URIs received in the Service-Route header field (during the last successful registration or re-registration). This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) return a 400 (Bad Request) response; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
  - b) replace the preloaded Route header field value in the request with the one received during the last registration in the Service-Route header field of the 200 (OK) response;
- 3) if the 200 (OK) response to the last REGISTER request, which created or refreshed the binding of the contact address from which the request is received, has not contained a Feature-Caps header field, specified in RFC 6809 [190] with a "+g.3gpp.atcf" header field parameter, then:
  - a) if the P-CSCF is located in the visited network, and local policy requires the application of IBCF capabilities in the visited network towards the home network, select an IBCF in the visited network and add the URI of the selected IBCF to the topmost Route header field;

NOTE 1: It is implementation dependent as to how the P-CSCF obtains the address of the IBCF exit point.

- 3A) if the 200 (OK) response to the last REGISTER request, which created or refreshed the binding of the contact address from which the request is received, contained a Feature-Caps header field with a "+g.3gpp.atcf" header field parameter, then:
  - a) add the ATCF URI for originating requests, that the P-CSCF used to forward the last REGISTER request which created or refreshed the binding of the contact address from which the request is received, to the topmost Route header field;
- 3B) if the request is originated from a UE which the P-CSCF considers as privileged sender, keep the P-Asserted-Identity header field unchanged if one was received, or include the originator of the request in the P-Asserted-Identity header field if no P-Asserted-Identity header field was received. In addition remove any P-Preferred-Identity header field, include the served user of the request in the P-Served-User header field as specified in RFC 5502 [133] and skip step 4) below;

NOTE 2: The P-CSCF determines if the UE is considered as privileged sender using the user-related policies provisioned to the P-CSCF (see subclause 5.2.1).

- 4) remove any P-Preferred-Identity header field or P-Asserted-Identity header field, if present, and insert P-Asserted-Identity header fields the value identifying the served user of the request and the value of the alternative identity of the originator of the request, if identified (see subclause 5.2.6.3.1), including the display name if previously stored during registration, representing the served user of the request;
- 4A) if the identity of the served user of the request was taken from P-Preferred-Identity header field by matching a registered wildcarded public user identity, and the identity of the served user is not a distinct identity within the range of the wildcarded public user identity, include the wildcarded public user identity value in the P-Profile-Key header field as defined in RFC 5002 [97];

NOTE 3: The matching of distinct public user identities takes precedence over the matching of wildcarded public user identities.

- 4B) if a P-Private-Network-Indication header field is included in the request, check whether the information saved during registration or from configuration allows the receipt of private network traffic from this source. If private network traffic is allowed, the P-CSCF shall check whether the received domain name in any included P-Private-Network-Indication header field in the request is the same as the domain name associated with that saved information. If private network traffic is not allowed, or the received domain name does not match, then the P-CSCF shall remove the P-Private-Network-Indication header field;
- 4C) if the served user of the request is understood from information saved during registration or from configuration to always send and receive private network traffic from this source, insert a P-Private-Network-Indication header field containing the domain name associated with that saved information;
- 5) add a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17];

before forwarding the request, based on the topmost Route header field, in accordance with the procedures of RFC 3261 [26].

#### 5.2.6.3.8 Responses to a request for a standalone transaction

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- 1) store the values received in the P-Charging-Function-Addresses header field;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

NOTE: The P-CSCF can find the IMS communication service supported for the standalone transaction, as determined by the originating home network, in the topmost occurrence of the "+g.3gpp.icsi-ref" header field parameter of the Feature-Caps header field(s) of 18x or 2xx response. The information can be used for charging purpose.

#### 5.2.6.3.9 Subsequent request other than a target refresh request

When the P-CSCF receives from the UE subsequent requests other than a target refresh request (including requests relating to an existing dialog where the method is unknown), the P-CSCF shall:

- 1) verify if the request relates to a dialog in which the originator of the request is involved:
  - a) if the request does not relate to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The P-CSCF will not forward the request. No other actions are required; or
  - b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;
- 1A) remove its own SIP URI from the top of the list of Route header fields;
- 2) verify that the resulting list of Route header fields matches the list of Record-Route header fields constructed by inverting the order of the stored list of Record-Route header fields and removing its Record-Route header field from the list. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) return a 400 (Bad Request) response; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or
  - b) replace the Route header field value in the request with the list of Record-Route header fields constructed by inverting the order of the stored list of Record-Route header fields and removing its Record-Route header field from the list;
- 3) for dialogs that are not INVITE dialogs, add a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17]; and
- 4) for INVITE dialogs, replace the saved CSeq header field value received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request (based on the topmost Route header field), in accordance with the procedures of RFC 3261 [26].

#### 5.2.6.3.10 Responses to a subsequent request other than a target refresh request

Void

#### 5.2.6.3.11 Request for an unknown method that does not relate to an existing dialog

When the P-CSCF receives from the UE the request for an unknown method (that does not relate to an existing dialog), and a service route value list exists for the served user of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header field (during the last successful registration or re-registration) is included, preserving the same order, as a subset of the preloaded Route header fields in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) return a 400 (Bad Request) response; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or
  - b) replace the Route header field value in the request with the one received during the last registration in the Service-Route header field of the 200 (OK) response;
- 2) if the 200 (OK) response to the last REGISTER request, which created or refreshed the binding of the contact address from which the request is received, has not contained a Feature-Caps header field, specified in RFC 6809 [190] with a "+g.3gpp.atcf" header field parameter, then:
  - a) if the P-CSCF is located in the visited network, and local policy requires the application of IBCF capabilities in the visited network towards the home network, then the P-CSCF shall select an IBCF in the visited network and add the URI of the selected IBCF to the topmost Route header field;

NOTE 1: It is implementation dependent as to how the P-CSCF obtains the address of the IBCF exit point.

- 2A) if the 200 (OK) response to the last REGISTER request, which created or refreshed the binding of the contact address from which the request is received, contained a Feature-Caps header field with a "+g.3gpp.atcf" header field parameter, then:
  - a) add the ATCF URI for originating requests, that the P-CSCF used to forward the last REGISTER request which created or refreshed the binding of the contact address from which the request is received, to the topmost Route header field;
- 2B) if the request is originated from a UE which the P-CSCF considers as privileged sender, keep the P-Asserted-Identity header field unchanged if one was received, or include the originator of the request in the P-Asserted-Identity header field if no P-Asserted-Identity header field was received. In addition remove any P-Preferred-Identity header field, include the served user of the request in the P-Served-User header field as specified in RFC 5502 [133] and skip step 3) below;

NOTE 2: The P-CSCF determines if the UE is considered privileged sender using based on the user-related policies provisioned to the P-CSCF (see subclause 5.2.1).

- 3) remove any P-Preferred-Identity header field or P-Asserted-Identity header field, if present, and insert a P-Asserted-Identity header fields the value identifying the originator of the request and the value of the alternative identity of the originator of the request, if identified (see subclause 5.2.6.3.1), including the display name if previously stored during registration, representing the served user of the request; and
- 3A) if the identity of the served user of the request was taken from P-Preferred-Identity header field by matching a registered wildcarded public user identity, and the identity of the served user is not a distinct identity within the range of the wildcarded public user identity, include the wildcarded public user identity value in the P-Profile-Key header field as defined in RFC 5002 [97];

NOTE 3: The matching of distinct public user identities takes precedence over the matching of wildcarded public user identities.

before forwarding the request, based on the topmost Route header field, in accordance with the procedures of RFC 3261 [26].



### 5.2.6.3.12 Responses to a request for an unknown method that does not relate to an existing dialog

NOTE: The P-CSCF can find the IMS communication service supported for the transaction, as determined by the originating home network, in the topmost occurrence of the "+g.3gpp.icsi-ref" header field parameter of the Feature-Caps header field(s) of 18x or 2xx response. The information can be used for charging purpose.

### 5.2.6.4 Requests terminated by the UE

#### 5.2.6.4.1 Void

#### 5.2.6.4.2 General for all responses

The P-CSCF shall forward the response to the UE using the mechanisms described in RFC 3261 [26] and RFC 3581 [56A], i.e. the P-CSCF shall send the response to the IP address indicated in the "received" header field parameter and, in case UDP is used, to the port indicated in the "rport" header field parameter (if present) of the Via header field associated with the UE. In case TCP is used, the P-CSCF shall use the TCP connection on which the REGISTER request was received for sending the response back to the UE.

#### 5.2.6.4.3 Initial request for a dialog

When the P-CSCF receives, destined for the UE, an initial request for a dialog, prior to forwarding the request, the P-CSCF shall:

- 1) if an indication has been received from the PCRF that the signalling bearer to the UE is lost, and has not recovered, reject the request by sending 503 (Service Unavailable) response);

NOTE 1: The signalling bearer can be considered as recovered by the P-CSCF when the registration timer expires in P-CSCF and the user is de-registered from the IM CN subsystem, a new REGISTER request from the UE is received providing an indication to the P-CSCF that the signalling bearer to that user has become available or a P-CSCF implementation dependent function which discovers that the signalling bearer is available to the UE.

NOTE 2: The Retry-After header field value is set based on operator policy.

- 2) convert the list of Record-Route header field values into a list of Route header field values and save this list of Route header fields;
- 3) if the request is an INVITE request, save a copy of the Contact, CSeq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;
- 4) if a security association or TLS session exists, when adding its own SIP URI to the top of the list of Record-Route header fields and save the list, build the P-CSCF SIP URI in a format that contains the protected server port number of the security association or TLS session established from the UE to the P-CSCF and either:
  - a) the P-CSCF FQDN that resolves to the IP address of the security association or TLS session established from the UE to the P-CSCF; or
  - b) the P-CSCF IP address of the security association or TLS session established from the UE to the P-CSCF;
- 5) if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is used, when adding its own SIP URI to the top of the list of Record-Route header fields and saving the list, build the P-CSCF URI in a format that contains an unprotected server port number where the P-CSCF expects subsequent requests from the UE;
- 6) if a security association or TLS session exists, when adding its own address to the top of the received list of Via header fields and save the list, build the P-CSCF Via header field entry in a format that contains the protected server port number of the security association or TLS session established from the UE to the P-CSCF and either:
  - a) the P-CSCF FQDN that resolves to the IP address of the security association or TLS session established from the UE to the P-CSCF; or
  - b) the P-CSCF IP address of the security association or TLS session established from the UE to the P-CSCF;

NOTE 3: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations or TLS session. For details of the usage of the two ports see 3GPP TS 33.203 [19].

- 7) if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is used, when adding its own address to the top of the received list of Via header fields and saving the list, build the P-CSCF Via header field entry in a format that contains an unprotected server port number where the P-CSCF expects responses to the current request from the UE;
- 7A) if the recipient of the request is understood from information saved during registration or from configuration to always send and receive private network traffic from this source, remove the P-Private-Network-Indication header field containing the domain name associated with that saved information;
- 8) store the values received in the P-Charging-Function-Addresses header field;
- 9) store the "icid-value" header field parameter received in the P-Charging-Vector header field; and
- 10) save a copy of the P-Called-Party-ID header field;

before forwarding the request to the UE either in accordance with the procedures of RFC 3261 [26] or as specified in RFC 5626 [92].

#### 5.2.6.4.4 Responses to an initial request for a dialog

When the P-CSCF receives any 1xx or 2xx response to the above request, the P-CSCF shall:

- 0A) if the response is originated from a UE which the P-CSCF considers as privileged sender, remove any P-Preferred-Identity header field, and skip step 1) below;

NOTE: The P-CSCF determines if the UE is considered privileged sender using based on the user-related policies provisioned to the P-CSCF (see subclause 5.2.1).

- 1) remove any P-Preferred-Identity header field or P-Asserted-Identity header field, if present, and insert a P-Asserted-Identity header field with the saved public user identity from the P-Called-Party-ID header field that was received in the request, plus the display name if previously stored during registration, representing the originator of the response;
- 2) verify that the list of Via header fields matches the saved list of Via header fields received in the request corresponding to the same dialog, including the P-CSCF Via header field value. This verification is done on a per Via header field value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) discard the response; or
  - b) replace the Via header field values with those received in the request;
- 3) verify that the list of URIs received in the Record-Route header field of the request corresponding to the same dialog is included, preserving the same order, as a subset of the Record-Route header field list of this response. This verification is done on a per URI basis, not as a whole string.

If the verification fails, then the P-CSCF shall either:

- a) discard the response; or
- b) replace the Record-Route header field values with those received in the request, and if a security association or TLS session exists, add its own Record-Route entry with its own SIP URI with the port number where it awaits subsequent requests from the calling party. The P-CSCF shall include in the Record-Route header field either:
  - the P-CSCF FQDN that resolves to its IP address; or
  - the P-CSCF IP address.

The P-CSCF shall remove the "comp" SIP URI parameter from the Record-Route header field.

If the verification is successful, the P-CSCF shall rewrite its own Record-Route entry to its SIP URI in a format that contains the port number where it awaits subsequent requests from the calling party. The P-CSCF shall include in the Record-Route header field either:

- a) the P-CSCF FQDN that resolves to its IP address; or
- b) the P-CSCF IP address.

The P-CSCF shall remove the "comp" SIP URI parameter from the Record-Route header field;

When adding its SIP URI to the Record-Route header field, the P-CSCF shall also copy the flow token and the "ob" SIP URI parameter from the Route header field of the initial dialog-forming request destined for the UE to its SIP URI, if the Route header field contained these values;

- 4) store the dialog ID and associate it with the private user identity and public user identity involved in the session; and
- 5) if the response corresponds to an INVITE request, save the Contact, To, From and Record-Route header field value received in the response such that the P-CSCF is able to release the session if needed. If the Contact header field in the response to the INVITE request contains a GRUU and the INVITE request was not sent over a bidirectional flow as defined in RFC 5626 [92], the P-CSCF shall save the GRUU received in the Contact header field of the response and associate that GRUU with the UE IP address and the UE port, for the security association on which the INVITE request was sent such that the P-CSCF is able to release the session if needed. The UE port used for the association is determined as follows:
  - if IMS AKA or SIP digest with TLS is being used as a security mechanism, the UE protected server port for the security association on which the request was received; or
  - if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled Authentication is being used as a security mechanism, the UE unprotected port on which the request was received;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

- 1) verify that the list of Via header fields matches the saved list of Via header fields received in the request corresponding to the same dialog, including the P-CSCF Via header field value. This verification is done on a per Via header field value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:
  - a) discard the response; or
  - b) replace the Via header field values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

#### 5.2.6.4.5 Target refresh request for a dialog

When the P-CSCF receives, destined for the UE, a target refresh request for a dialog, prior to forwarding the request, the P-CSCF shall:

- 1) if a security association or TLS session exists, add its own address to the top of the received list of Via header fields and save the list. The P-CSCF Via header field entry is built in a format that contains the protected server port number of the security association or TLS session established from the UE to the P-CSCF and either:
  - a) the P-CSCF FQDN that resolves to the IP address of the security association or TLS session established from the UE to the P-CSCF; or
  - b) the P-CSCF IP address of the security association or TLS session established from the UE to the P-CSCF;

NOTE 1: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations or TLS session. For details of the usage of the two ports see 3GPP TS 33.203 [19].

- 2) if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is used, when adding its own address to the top of the received list of Via header fields and saving the list, build the P-CSCF Via header field entry in a format that contains an unprotected server port number where the P-CSCF expects responses to the current request from the UE;
- 3) if a security association or TLS session exists, when adding its own SIP URI to the top of the list of Record-Route header fields and save the list, build the P-CSCF SIP URI in a format that contains the protected server port number of the security association or TLS session established from the UE to the P-CSCF and either:

- a) the P-CSCF FQDN that resolves to the IP address of the security association or TLS session established from the UE to the P-CSCF; or
  - b) the P-CSCF IP address of the security association or TLS session established from the UE to the P-CSCF;
- 4) if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is used, when adding its own SIP URI to the top of the list of Record-Route header fields and saving the list, build the P-CSCF URI in a format that contains an unprotected server port number where the P-CSCF expects subsequent requests from the UE; and
  - 5) for INVITE dialogs, replace the saved Contact and CSeq header field values received in the request such that the P-CSCF is able to release the session if needed;

NOTE 2: The replaced Contact header field value is valid only if a 1xx or 2xx response will be received for the request. In other cases the old value is still valid.

before forwarding the request to the UE in accordance with the procedures of either RFC 3261 [26] or RFC 5626 [92].

#### 5.2.6.4.6 Responses to a target refresh request for a dialog

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) verify that the list of Via header fields matches the saved list of Via header fields received in the request corresponding to the same dialog, including the P-CSCF Via header field value. This verification is done on a per Via header field value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) discard the response; or
  - b) replace the Via header field values with those received in the request;
- 2) if a security association or TLS session exists, rewrite its own Record-Route entry to the same value as for the response to the initial request for the dialog and remove the "comp" SIP URI parameter;
- 3) replace the saved Contact header field value received in the response such that the P-CSCF is able to release the session if needed. If the Contact header field in the response to the target refresh request for a dialog contains a GRUU and target refresh request for a dialog was not sent over a bidirectional flow, the P-CSCF shall save the GRUU received in the Contact header field of the response and associate That GRUU with the UE IP address and the UE port, for the security association on which the target refresh request for a dialog was sent such that the P-CSCF is able to release the session if needed. The UE port used for the association is determined as follows:
  - if IMS AKA or SIP digest with TLS is being used as a security mechanism, the UE protected server port for the security association on which the request was received; or
  - if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled Authentication is being used as a security mechanism, the UE unprotected port on which the request was received; and
- 4) if the P-CSCF inserted the header field parameters into the Feature-Caps header field of the initial request for the dialog then when the response is forwarded in the same direction, the P-CSCF shall insert the header field parameters with the same parameter values in the Feature-Caps header field;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

- 1) verify that the list of Via header fields matches the saved list of Via header fields received in the request corresponding to the same dialog, including the P-CSCF Via header field value. This verification is done on a per Via header field value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:
  - a) discard the response; or
  - b) replace the Via header field values with those received in the request; and
- 2) if a security association or TLS session exists, rewrite the IP address and the port number of its own Record-Route entry to the IP address and the port number where it awaits subsequent requests from the calling party and remove the "comp" SIP URI parameter;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

#### 5.2.6.4.7 Request for a standalone transaction

When the P-CSCF receives, destined for the UE, a request for a standalone transaction, or a request for an unknown method (that does not relate to an existing dialog), prior to forwarding the request, the P-CSCF shall:

- 1) if an indication has been received from the PCRF that the signalling bearer to the UE is lost, and has not recovered, reject the request by sending 503 (Service Unavailable) response;

NOTE 1: The signalling bearer can be considered as recovered by the P-CSCF when the registration timer expires in P-CSCF and the user is de-registered from the IM CN subsystem, a new REGISTER request from the UE is received providing an indication to the P-CSCF that the signalling bearer to that user has become available or a P-CSCF implementation dependent function which discovers that the signalling bearer is available to the UE.

NOTE 2: The Retry-After header field value is set based on operator policy.

- 2) if a security association or TLS session exists, add its own address to the top of the received list of Via header fields and save the list. The P-CSCF Via header field entry is built in a format that contains the protected server port number of the security association or TLS session established from the UE to the P-CSCF and either:
  - a) the P-CSCF FQDN that resolves to the IP address of the security association or TLS session established from the UE to the P-CSCF; or
  - b) the P-CSCF IP address of the security association or TLS session established from the UE to the P-CSCF;

NOTE 3: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations or TLS session. For details of the usage of the two ports see 3GPP TS 33.203 [19].

- 3) if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is used, when adding its own address to the top of the received list of Via header fields and saving the list, build the P-CSCF Via header field entry in a format that contains an unprotected server port number where the P-CSCF expects responses to the current request from the UE;
- 3A) if the recipient of the request is understood from information saved during registration or from configuration to always send and receive private network traffic from this source, remove the P-Private-Network-Indication header field containing the domain name associated with that saved information;
- 4) store the values received in the P-Charging-Function-Addresses header field;
- 5) store the "icid-value" header field parameter received in the P-Charging-Vector header field; and
- 6) save a copy of the P-Called-Party-ID header field;

before forwarding the request to the UE either in accordance with the procedures of RFC 3261 [26] or as specified in RFC 5626 [92].

#### 5.2.6.4.8 Responses to a request for a standalone transaction

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- 1) verify that the list of Via header fields matches the saved list of Via header fields received in the request corresponding to the same dialog, including the P-CSCF Via header field value. This verification is done on a per Via header field value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:
  - a) discard the response; or
  - b) replace the Via header field values with those received in the request;
- 1A) if the response is originated from a UE which the P-CSCF considers as privileged sender, remove any P-Preferred-Identity header field, and skip step 2) below; and

NOTE: The P-CSCF determines if the UE is considered privileged sender using based on the user-related policies provisioned to the P-CSCF (see subclause 5.2.1).

- 2) remove any P-Preferred-Identity header field or P-Asserted-Identity header field, if present, and insert an P-Asserted-Identity header field with the saved public user identity from the P-Called-Party-ID header field of the request, plus the display name if previously stored during registration, representing the originator of the response;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

#### 5.2.6.4.9 Subsequent request other than a target refresh request

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a target refresh request (including requests relating to an existing dialog where the method is unknown), prior to forwarding the request, the P-CSCF shall:

- 1) if a security association or TLS session exists, add its own address to the top of the received list of Via header fields and save the list. The P-CSCF Via header field entry is built in a format that contains the protected server port number of the security association or TLS session established from the UE to the P-CSCF and either:
  - a) the P-CSCF FQDN that resolves to the IP address of the security association or TLS session established from the UE to the P-CSCF; or
  - b) the P-CSCF IP address of the security association or TLS session established from the UE to the P-CSCF;

NOTE: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations or TLS session. For details of the usage of the two ports see 3GPP TS 33.203 [19].

- 2) if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is used, when adding its own address to the top of the received list of Via header fields and saving the list, build the P-CSCF Via header field entry in a format that contains an unprotected server port number where the P-CSCF expects responses to the current request from the UE;
- 3) store the "icid-value" header field parameter from P-Charging-Vector header field; and
- 4) for INVITE dialogs, replace the saved CSeq header field value received in the request such that the P-CSCF is able to release the session if needed;

before forwarding the request to the UE either in accordance with the procedures of RFC 3261 [26] or as specified in RFC 5626 [92].

#### 5.2.6.4.10 Responses to a subsequent request other than a target refresh request

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- 1) verify that the list of Via header fields matches the saved list of Via header fields received in the request corresponding to the same dialog, including the P-CSCF Via header field value. This verification is done on a per Via header field value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:
  - a) discard the response; or
  - b) replace the Via header field values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

#### 5.2.6.4.11 Request for an unknown method that does not relate to an existing dialog

Void.

#### 5.2.6.4.12 Responses to a request for an unknown method that does not relate to an existing dialog

Void.

## 5.2.7 Initial INVITE

### 5.2.7.1 Introduction

In addition to following the procedures for initial requests defined in subclause 5.2.6, initial INVITE requests also follow the procedures of this subclause.

### 5.2.7.2 UE-originating case

When the P-CSCF receives from the UE an INVITE request for which resource authorization procedure is required, if it receives from the IP-CAN (e.g. via PCRF) an indication that the requested resources for the multimedia session being established cannot be granted and this indication does not provide an acceptable bandwidth information, the P-CSCF shall return a 503 (Service Unavailable) response to the received INVITE request. Depending on local operator policy, this 503 (Service Unavailable) response may include a Retry-After header indicating how long the UE shall wait before it can reattempt the request.

When the P-CSCF receives from the UE an INVITE request, the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

The P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

If received from the IP-CAN, the P-CSCF shall also include the access-network-charging-info parameter (e.g. received via the PCRF, over the Rx or Gx interfaces) in the P-Charging-Vector header field in the first request originated by the UE that traverses the P-CSCF, as soon as the charging information is available in the P-CSCF, e.g., after the local resource reservation is complete. Typically, this first request is an UPDATE request if the remote UA supports the "integration of resource management in SIP" extension or a re-INVITE request if the remote UA does not support the "integration of resource management in SIP" extension. See subclause 5.2.7.4 for further information on the access network charging information.

If:

- the UE is roaming;
- the P-CSCF is not in the home network; and
- an agreement exists with the home network operator (as identified by the bottom most URI in the list of URIs received in the Service-Route header field during the last successful registration or re-registration) to support Roaming Architecture for Voice over IMS with Local Breakout;

the P-CSCF may insert into the request a Feature-Caps header field with the "+g.3gpp.trf" header field parameter as specified in RFC 6809 [190]. Based on local policy the P-CSCF shall insert the "+g.3gpp.trf" header field parameter with the parameter value set to the URI of the desired TRF.

If:

- the UE is roaming;
- the P-CSCF is not in the home network; and
- the visited network supports MRB functionality for the allocation of MRF resources and if an agreement exists with the home operator (identified by the bottom most URI in the list of URIs received in the Service-Route header field during the last successful registration or re-registration) to provide access to MRF resources from the visited network;

the P-CSCF may insert into the request a Feature-Caps header field with the "+g.3gpp.mrb" header field parameter, as specified in RFC 6809 [190]. Based on local policy the P-CSCF shall insert the "+g.3gpp.mrb" header field parameter with the parameter value set to the URI of the desired MRB.

The P-CSCF (IMS-ALG) shall transparently forward a received Contact header field towards the UE when the Contact header field contains a GRUU or a media feature tag indicating a capability for which the URI can be used.

NOTE 2: One example of such a media feature tag is the isfocus media feature tag where the URI in the Contact header field is used by conference services to transport the temporary conference identity that can be used when rejoining an ongoing conference.

NOTE 3: Various mechanisms can be applied to recognize the need for priority treatment (e.g., based on the dialled digits). The exact mechanisms are left to national regulation and network configuration.

Based on the alternative mechanism to recognize the need for priority treatment, the P-CSCF shall insert the temporarily authorised Resource-Priority header field with appropriate namespace and priority value in the INVITE request.

### 5.2.7.3 UE-terminating case

When the P-CSCF receives an INVITE request destined for the UE the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, then the P-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it in order to make it work.

When the P-CSCF receives an initial INVITE request destined for the UE, it will have a list of Record-Route header fields. Prior to forwarding the initial INVITE request, the P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

If received from the IP-CAN, the P-CSCF shall also include the access-network-charging-info parameter (e.g. received via the PCRF, over the Rx or Gx interfaces) in the P-Charging-Vector header field in the first request or reliable response originated by the UE that traverses the P-CSCF, as soon as the charging information is available in the P-CSCF e.g., after the local resource reservation is complete. See subclause 5.2.7.4 for further information on the access network charging information.

If the user-related policies provisioned to the P-CSCF (see subclause 5.2.1) do not indicate the served UE is authorized to send early media, the P-CSCF shall not allow media flows in forward and backward direction before the 200 (OK) response to the initial INVITE is received.

If the user-related policies provisioned to the P-CSCF (see subclause 5.2.1) indicate that the served UE is authorized to send early media, the P-CSCF shall not remove the P-Early-Media header field if received in a 18x provisional response or in an UPDATE request.

The P-CSCF (IMS-ALG) shall transparently forward a received Contact header field towards the UE when the Contact header field contains a GRUU or a media feature tag indicating a capability for which the URI can be used.

NOTE 2: One example of such a media feature tag is the isfocus media feature tag where the URI in the Contact header field is used by conference services to transport the temporary conference identity that can be used when rejoining an ongoing conference.

### 5.2.7.4 Access network charging information

The P-CSCF shall include the "access-network-charging-info" header field parameter within the P-Charging-Vector header field as described in subclause 7.2A.5.

## 5.2.8 Call release

### 5.2.8.1 P-CSCF-initiated call release

#### 5.2.8.1.1 Cancellation of a session currently being established

Upon receipt of an indication that radio/bearer resources is no longer available for a media negotiated in a multimedia session currently being established (e.g. an Rx interface message from PCRF) and if no SIP message removing the media for which resources are no longer available is received within an operator defined time after the reception of the indication, the P-CSCF shall cancel that dialog by applying the following steps:



- 1) if the P-CSCF serves the calling user of the session, send out a CANCEL request to cancel the INVITE request towards the terminating UE that includes a Reason header field containing a 503 (Service Unavailable) status code according to the procedures described in RFC 3261 [26] and RFC 3326 [34A]; and
- 2) if the P-CSCF serves the called user of the session, send out a 503 (Service Unavailable) response to the received INVITE request.

Upon receipt of an indication that QoS or bearer resources are no longer available for a media negotiated in a multimedia session currently being established (e.g. an Rx interface message from PCRF) and if no SIP message removing the media for which resources are no longer available is received within an operator defined time after the reception of the indication, the P-CSCF shall cancel that dialog by responding to the original INVITE request with a 503 (Service Unavailable) response, and by sending out a CANCEL request to the INVITE request towards the terminating UE that includes a Reason header field containing a 503 (Service Unavailable) status code according to the procedures described in RFC 3261 [26] and RFC 3326 [34A].

### 5.2.8.1.2 Release of an existing session

Upon:

- 1) receipt of an indication that the radio/bearer resources are no longer available for a media negotiated in a session (e.g. an Rx interface message from PCRF) and if no SIP message removing the media for which resources are no longer available is received within an operator defined time after the reception of the indication;
- 2) receipt of an indication that the signalling bearer is no longer available (e.g. an Rx interface message from PCRF); or
- 3) detecting that the SDP offer conveyed in a SIP response contained parameters which are not allowed according to the local policy (as specified in the subclause 6.2);

the P-CSCF shall release the respective dialog by applying the following steps:

- 1) if the P-CSCF serves the calling user of the session, then the P-CSCF shall generate a BYE request destined for the called user based on the information saved for the related dialog, including:
  - a Request-URI, set to the stored Contact header field provided by the called user;
  - a To header field, set to the To header field value as received in the 200 (OK) response for the initial INVITE request;
  - a From header field, set to the From header field value as received in the initial INVITE request;
  - a Call-ID header field, set to the Call-Id header field value as received in the initial INVITE request;
  - a CSeq header field, set to the current CSeq value stored for the direction from the calling to the called user, incremented by one;
  - a Route header field, set to the routing information towards the called user as stored for the dialog;
  - a Reason header field that contains:
    - a 503 (Service Unavailable) response code, if radio/bearer interface resources are no longer available; or
    - a 503 (Service Unavailable) response code, if the signalling bearer is no longer available; or
    - a 488 (Not Acceptable Here) response code, if a SDP offer conveyed in a SIP response contained parameters which are not allowed according to the local policy;
  - further header fields, based on local policy; and
  - send the generated BYE requests towards the called user;
- 2) if the P-CSCF serves the calling user of the session and upon detecting that the SDP offer conveyed in a SIP response contained parameters which are not allowed according to the local policy (as specified in the subclause 6.2), then the P-CSCF shall generate an additional BYE request destined for the calling user based on the information saved for the related dialog, including:

- a Request-URI, set to a contact address obtained from the stored Contact header field if provided by the calling user. If the stored Contact header field contains either a public or a temporary GRUU, the P-CSCF shall set the Request-URI either to:
    - a) the stored UE IP address and the UE port associated with the respective GRUU, if the stored Contact header field contains either a public or a temporary GRUU and the bidirectional flow as defined in RFC 5626 [92] is not used for this session; or
    - b) the UE IP address and UE port associated with the bidirectional flow that the P-CSCF uses to send the in-dialog requests toward the UE as defined in RFC 5626 [92];
  - a To header field, set to the From header field value as received in the initial INVITE request;
  - a From header field, set to the To header field value as received in the 200 (OK) response for the initial INVITE request;
  - a Call-ID header field, set to the Call-Id header field value as received in the initial INVITE request;
  - a CSeq header field, set to the current CSeq value stored for the direction from the called to the calling user, incremented by one;
  - a Route header field, set to the routing information towards the calling user as stored for the dialog;
  - a Reason header field that contains a 488 (Not Acceptable Here) response code;
  - further header fields, based on local policy; and
  - send the BYE request either:
    - a) to the contact address indicated in the Request-URI, if the dialog being released did not use the bidirectional flow to send the requests to the UE as defined in RFC 5626 [92]; or
    - b) over the same flow that the P-CSCF uses to send the in-dialog requests toward the UE as defined in RFC 5626 [92];
- 3) If the P-CSCF serves the called user of the session, then the P-CSCF shall generate a BYE request destined for the calling user based on the information saved for the related dialog, including:
- a Request-URI, set to the stored Contact header field provided by the calling user;
  - a To header field, set to the From header field value as received in the initial INVITE request;
  - a From header field, set to the To header field value as received in the 200 (OK) response for the initial INVITE request;
  - a Call-ID header field, set to the Call-Id header field value as received in the initial INVITE request;
  - a CSeq header field, set to the current CSeq value stored for the direction from the called to the calling user, incremented by one;
  - a Route header field, set to the routing information towards the calling user as stored for the dialog;
  - a Reason header field that contains:
    - a 503 (Service Unavailable) response code, if radio/bearer interface resources are no longer available; or
    - a 488 (Not Acceptable Here) response code, if SDP payload contained parameters which are not allowed according to the local policy;
  - further header fields, based on local policy; and
  - send the generated BYE requests towards the calling user;
- 4) if the P-CSCF serves the called user of the session and upon detecting that the SDP offer conveyed in a SIP response contained parameters which are not allowed according to the local policy (as specified in the subclause 6.2), then the P-CSCF shall generate an additional BYE request destined for the called user based on the information saved for the related dialog, including:

- a Request-URI, set to a contact address obtained from the stored Contact header field if provided by the called user. If the stored Contact header field contains either a public or a temporary GRUU, the P-CSCF shall set the Request-URI either to:
  - a) the stored UE IP address and the UE port associated with the respective GRUU, if the stored Contact header field contains either a public or a temporary GRUU and the bidirectional flow as defined in RFC 5626 [92] is not used for this session; or
  - b) the UE IP address and the UE port associated with the bidirectional flow that the P-CSCF uses to send the in-dialog requests toward the UE as defined in RFC 5626 [92];
- a To header field, set to the To header field value as received in the 200 (OK) response for the initial INVITE request;
- a From header field, set to the From header field value as received in the initial INVITE request;
- a Call-ID header field, set to the Call-Id header field value as received in the initial INVITE request;
- a CSeq header field, set to the current CSeq value stored for the direction from the calling to the called user, incremented by one;
- a Route header field, set to the routing information towards the called user as stored for the dialog;
- a Reason header field that contains a 488 (Not Acceptable Here) response code;
- further header fields, based on local policy; and
- send the BYE request either:
  - a) to the contact address indicated in the Request-URI, if the dialog being released did not use the bidirectional flow to send the requests to the UE as defined in RFC 5626 [92]; or
  - b) over the same flow that the P-CSCF uses to send the in-dialog requests toward the UE as defined in RFC 5626 [92].

Upon receipt of the 2xx responses for the BYE requests, the P-CSCF shall delete all information related to the dialog and the related multimedia session.

#### 5.2.8.1.3 Abnormal cases

Upon receipt of a request on a dialog for which the P-CSCF initiated session release, the P-CSCF shall terminate this received request and answer it with a 481 (Call/Transaction Does Not Exist) response.

#### 5.2.8.1.4 Release of the existing dialogs due to registration expiration and deletion of the security association, IP association or TLS session

If there are still active dialogs associated with the user after the security associations, IP association or TLS sessions were deleted, the P-CSCF shall discard all information pertaining to these dialogs without performing any further SIP transactions with the peer entities of the P-CSCF.

NOTE: If the interface between the P-CSCF and the IP-CAN is supported, the P-CSCF will also indicate (e.g. via the Rx or Gx interface) that the session has been terminated.

#### 5.2.8.2 Call release initiated by any other entity

When the P-CSCF receives a 2xx response for a BYE request matching an existing dialog, then the P-CSCF shall delete all the stored information related to the dialog.

#### 5.2.8.3 Session expiration

If the P-CSCF requested the session to be refreshed periodically, and the P-CSCF got the indication that the session will be refreshed, when the session timer expires, the P-CSCF shall delete all the stored information related to the dialog.

NOTE: If the interface between the P-CSCF and the IP-CAN is supported, the P-CSCF will also indicate to the IP-CAN (e.g. via the Rx or Gx interface), that the session has terminated.

## 5.2.9 Subsequent requests

### 5.2.9.1 UE-originating case

The P-CSCF shall respond to all reINVITE requests with a 100 (Trying) provisional response.

For a reINVITE request or UPDATE request from the UE within the same dialog, the P-CSCF shall include the updated access-network-charging-info parameter from P-Charging-Vector header field when sending the SIP request to the S-CSCF. See subclause 5.2.7.4 for further information on the access network charging information.

For an ACK request from the UE sent on a dialog where a 200 (OK) has been received, the P-CSCF shall include the access-network-charging-info parameter from the P-Charging-Vector header field when updated access-network-charging-info is available when sending the ACK request to the S-CSCF. See subclause 5.2.7.4 for further information on the access network charging information.

### 5.2.9.2 UE-terminating case

The P-CSCF shall respond to all reINVITE requests with a 100 (Trying) provisional response.

For a reINVITE request or UPDATE request destined towards the UE within the same dialog, when the P-CSCF sends 200 (OK) response (to the INVITE request or UPDATE request) towards the S-CSCF, the P-CSCF shall include the updated access-network-charging-info parameter in the P-Charging-Vector header field. See subclause 5.2.7.4 for further information on the access network charging information.

## 5.2.10 Emergency service

### 5.2.10.1 General

If the P-CSCF belongs to a network where the registration is not required to obtain emergency service, the P-CSCF shall accept any unprotected request on the IP address and port advertised to the UE during the P-CSCF discovery procedure. The P-CSCF shall also accept any unprotected request on the same IP address and the default port as specified in RFC 3261 [26].

When the P-CSCF sends unprotected responses to the UE, it shall use the same IP address and port where the corresponding request was received.

The P-CSCF can handle emergency session and other requests from both a registered user as well as an unregistered user. Certain networks only allow emergency session from registered users.

NOTE 1: If only emergency setup from registered users is allowed, a request from an unregistered user is ignored since it is received outside of the security association, TLS session or IP association.

The P-CSCF can handle emergency session establishment within a non-emergency registration, i.e. one that did not contain the "sos" SIP URI parameter in the Contact header field of the 200 (OK) response.

If the network uses the Resource-Priority header field to give control the priority of emergency calls, and the P-CSCF receives a REGISTER request containing an "sos" SIP URI parameter in the Contact header field, the P-CSCF shall, in addition to the normal handling of the REGISTER request, add a Resource-Priority header field containing a namespace of "esnet" as defined in RFC 7135 [197] to the REGISTER request.

Upon receiving the 200 (OK) response to the REGISTER request that completes the emergency registration, as identified by the presence of the "sos" SIP URI parameter in the Contact header field of the 200 (OK) response, the P-CSCF shall not subscribe to the registration event package for any emergency public user identity specified in the REGISTER request.

The P-CSCF shall store a configurable list of local emergency service identifiers, i.e. emergency numbers (the emergency numbers that can be resolved in the network to which the P-CSCF belongs) and the emergency service URNs. In addition to that, the P-CSCF shall store a configurable list of roaming partners' emergency service identifiers.

NOTE 2: The emergency service URN is common to all networks, although subtypes might either not necessarily be in use, or a different set of subtypes is in use in different networks.

Access technology specific procedures are described in each access technology specific annex to determine the originating network of the requests.

NOTE 3: Depending on local operator policy, the P-CSCF has the capability to reject requests relating to specific methods in accordance with RFC 3261 [26], as an alternative to the functionality described above.

### 5.2.10.2 General treatment for all dialogs and standalone transactions excluding the REGISTER method – requests from an unregistered user

If the P-CSCF receives an initial request for a dialog or standalone transaction, or an unknown method from an unregistered user on the IP address and the unprotected port advertised to the UE during the P-CSCF discovery or the SIP default port, the P-CSCF shall inspect the Request-URI independent of values of possible entries in the received Route header fields for emergency service identifiers. The P-CSCF shall consider the Request URI of the initial request as a emergency service identifier, if it is an emergency number or an emergency service URN in the list of local emergency service identifiers or in the list of roaming partners emergency service identifiers.

If the P-CSCF detects that the Request-URI of the initial request for a dialog or a standalone transaction, or an unknown method matches one of the emergency service identifiers, the P-CSCF shall:

- 1) include in the Request-URI an emergency service URN, i.e. a service URN with a top-level service type of "sos" in accordance with RFC 5031 [69]:
  - if the received Request-URI matches an emergency service URN, as received in the Request-URI from the UE; and
  - if the received Request-URI does not match an emergency service URN, as deduced from the Request-URI received from the UE;

- 2) include a topmost Route header field set to the URI associated with an E-CSCF;

NOTE: How the list of E-CSCF is obtained by the P-CSCF is implementation dependent.

- 3) execute the procedure described in subclause 5.2.6.3.3, subclause 5.2.6.3.7, subclause 5.2.6.3.11 and subclause 5.2.7.2, as appropriate except for:
  - verifying the preloaded route against the received Service-Route header field;
  - routing to IBCF;
  - removing the P-Preferred-Identity header field; and
  - inserting a P-Asserted-Identity header field;
- 3A) insert a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17];
- 3B) where the network uses the Resource-Priority header field to give control the priority of emergency calls, add a Resource-Priority header field containing a namespace of "esnet" as defined in RFC 7135 [197]; and
- 4) if the P-CSCF detects that the UE is behind a NAT, and the UE's Via header field contains a "keep" header field parameter, the P-CSCF shall add a value to the parameter, to indicate that it is willing to receive keep-alives associated with the dialog from the UE, as defined in RFC 6223 [143].

When the P-CSCF receives any 1xx or 2xx response to the above requests, the P-CSCF shall execute the appropriate procedure for the type of request described in subclause 5.2.6.3.4, subclause 5.2.6.3.8, and subclause 5.2.6.3.12, except that the P-CSCF may rewrite the port number of its own Record-Route entry to an unprotected port where the P-CSCF wants to receive the subsequent incoming requests from the UE belonging to this dialog.

If the P-CSCF does not receive any response to the initial request for a dialog or standalone transaction or unknown method (including its retransmissions); or receives a 3xx response or 480 (Temporarily Unavailable) response to an initial request for a dialog or standalone transaction or an unknown method, the P-CSCF shall include a URI associated with a different E-CSCF in the topmost Route header field and forward the request.

When the P-CSCF received a subsequent request in the dialog from the UE, and the network uses the Resource-Priority header field to control the priority of emergency calls, the P-CSCF shall add a Resource-Priority header field containing a namespace of "esnet" as defined in RFC 7135 [197].

When the P-CSCF receives a target refresh request from the UE for a dialog, the P-CSCF shall execute the procedure described in subclause 5.2.6.3.5.

When the P-CSCF receives from the UE subsequent requests other than a target refresh request (including requests relating to an existing dialog where the method is unknown), the P-CSCF shall execute the procedure described in subclause 5.2.6.3.9.

When the P-CSCF receives any 1xx or 2xx response to the above requests, the P-CSCF shall execute the appropriate procedure for the type of request described in subclause 5.2.6.3.5 or subclause 5.2.6.3.9.

### 5.2.10.2A General treatment for all dialogs and standalone transactions excluding the REGISTER method – requests to an unregistered user

When the P-CSCF receives, destined for the UE, a target refresh request for a dialog, prior to forwarding the request, the P-CSCF shall execute the procedure described in step 5, the paragraph of subclause 5.2.6.4.5.

When the P-CSCF receives a 1xx or 2xx response to the above request the P-CSCF shall execute the procedure described in subclause 5.2.6.4.6.

When the P-CSCF receives any other response to the above request the P-CSCF shall execute the procedure described in step 1) to 2) in the paragraph of subclause 5.2.6.4.6 describing when the P-CSCF receives any other response to a target request.

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a target refresh request (including requests relating to an existing dialog where the method is unknown), prior to forwarding the request, the P-CSCF shall execute the procedure described in steps 3 and 4 of subclause 5.2.6.4.9 describing when a P-CSCF receives a subsequent request.

When the P-CSCF receives any other response to the above request the P-CSCF shall execute the procedure described in step 1 in the paragraph of subclause 5.2.6.4.10 describing when the P-CSCF receives any other response to a subsequent request.

### 5.2.10.3 General treatment for all dialogs and standalone transactions excluding the REGISTER method after emergency registration

If the P-CSCF receives an initial request for a dialog, or a standalone transaction, or an unknown method, for a registered user over the security association, TLS session, or IP association that was created during the emergency registration, as identified by the presence of the "sos" SIP URI parameter in the Contact header field of the 200 (OK) response, the P-CSCF shall inspect the Request-URI independent of values of possible entries in the received Route header fields for emergency service identifiers. The P-CSCF shall consider the Request URI of the initial request as an emergency service identifier, if it is an emergency number or an emergency service URN from the configurable lists that are associated with:

- the country of the operator to which the P-CSCF belongs to; and
- for inbound roamers, the country from which the UE is roaming from. The P-CSCF determines the country to which the UE is belonging to based on the content of the P-Asserted-Identity header field which contains the home network domain name in a SIP URI belonging to the user.

If the P-CSCF detects that the Request-URI of the initial request for a dialog, or a standalone transaction, or an unknown method does not match any one of the emergency service identifiers in the associated lists, the P-CSCF shall reject the request by returning a 403 (Forbidden) response to the UE.

If the P-CSCF detects that the Request-URI of the initial request for a dialog, or a standalone transaction, or an unknown method matches one of the emergency service identifiers in the associated lists, the P-CSCF shall:

- 1) include in the Request-URI an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]:
  - if the received Request-URI matches an emergency service URN, as received from the UE in the Request-URI; and
  - if the received Request-URI does not match an emergency service URN, as deduced from the Request-URI received from the UE.
- 1A) if the operator policy requires that emergency service requests are forwarded to the S-CSCF and the P-CSCF determines that the network to which the originating user is attached (see the IP-CAN specific annexes for the detailed procedure) is the network the P-CSCF is in and the user is not a roaming user then:

NOTE 1: The P-CSCF can know if the user is roaming by comparing the home domain name of the user received in the Request-URI in the REGISTER request with its own domain name. If they are different the user is a roaming user.

- a) execute the procedure described in subclause 5.2.6.3.3, subclause 5.2.6.3.7, subclause 5.2.6.3.11 and subclause 5.2.7.2, as appropriate except for routing to IBCF;
- b) before the request is forwarded in the referenced procedures, include a bottom most Route header field set to the URI associated with an E-CSCF;

NOTE 2: It is implementation dependent as to how the P-CSCF obtains the list of E-CSCFs.

1B) if the condition for 1A) is not fulfilled then:

- a) execute the procedure described in subclause 5.2.6.3.3, subclause 5.2.6.3.7, subclause 5.2.6.3.11 and subclause 5.2.7.2, as appropriate except for verifying the preloaded route against the received Service-Route header field; and routing to IBCF;
- b) before the request is forwarded in the referenced procedures, remove all Route header fields and include a Route header field set to the URI associated with an E-CSCF; and

NOTE 3: It is implementation dependent as to how the P-CSCF obtains the list of E-CSCFs.

- 1C) if the request is from a UE that is not considered as privileged sender and if the alternative identity of the originator of the request was not identified (see subclause 5.2.6.3.1):
  - i) if the P-Asserted-Identity header field in the request to be sent contains a SIP URI and if a tel URI belongs to the set of implicitly registered public user identities that contains the SIP URI, add a second P-Asserted-Identity header field that contains the first tel URI of the implicitly registered public user identities; and
  - ii) if the P-Asserted-Identity header field in the request to be sent contains a tel URI, add a second P-Asserted-Identity header field that contains the first SIP URI of the implicitly registered public user identities that contains the tel URI;
- 2) if the request contains a Contact header field containing a GRUU the P-CSCF shall save the GRUU received in the Contact header field of the request and associate it with the UE IP address and UE port such that the P-CSCF is able to route target refresh request containing that GRUU in the Request-URI. The UE port used for the association is determined as follows:
  - if IMS AKA or SIP digest with TLS is being used as a security mechanism, the UE protected server port for the security association on which the request was received; or
  - if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled Authentication is being used as a security mechanism, the UE unprotected port on which the request was received; and
- 3) where the network uses the Resource-Priority header field to control the priority of emergency calls, add a Resource-Priority header field containing a namespace of "esnet" as defined in RFC 7135 [197].

If the P-CSCF does not receive any response to an initial request for a dialog or standalone transaction or an unknown method sent to an E-CSCF (including its retransmissions); or receives a 480 (Temporarily Unavailable) response to an initial request for a dialog or standalone transaction or an unknown method sent to an E-CSCF, the P-CSCF shall include a URI, associated with a different E-CSCF, in the topmost Route header field and forward the request.

If the P-CSCF does not receive any response to an initial request for a dialog or standalone transaction or an unknown method sent to a S-CSCF (including its retransmissions); or receives a 480 (Temporarily Unavailable) response to an initial request for a dialog or standalone transaction or an unknown method sent to a S-CSCF, the P-CSCF shall include a URI, associated with a different E-CSCF, in the topmost Route header field of the initial request for a dialog or standalone transaction or an unknown method, and forward the request.

When the P-CSCF received a subsequent request in the dialog from the UE, and the network uses the Resource-Priority header field to control the priority of emergency calls, the P-CSCF shall add a Resource-Priority header field containing a namespace of "esnet" as defined in RFC 7135 [197].

When the P-CSCF receives a target refresh request for a dialog with the Request-URI containing a GRUU the P-CSCF shall:

- obtain the UE IP address and UE port associated to the GRUU contained in the Request-URI and rewrite the Request-URI with that UE IP address and UE port; and
- perform the steps in subclause 5.2.6.4.5 for when the P-CSCF receives, destined for the UE, a target refresh request for a dialog.

#### 5.2.10.4 General treatment for all dialogs and standalone transactions excluding the REGISTER method - non-emergency registration

If the P-CSCF receives an initial request for a dialog, or a standalone transaction, or an unknown method, for a registered user, and the request is:

- a) understood from saved or included information to relate to private network traffic (see subclause 5.2.6.3), and operator policy requires the P-CSCF to detect an emergency session request relating to private network traffic; or
- b) not understood from saved or included information to relate to private network traffic (see subclause 5.2.6.3);

then the P-CSCF shall inspect the Request-URI independent of values of possible entries in the received Route header fields for emergency service identifiers. The P-CSCF shall consider the Request URI of the initial request as an emergency service identifier, if it is an emergency numbers or an emergency service URN from the configurable lists that are associated with:

- the country of the operator to which the P-CSCF belongs to;
- for inbound roamers, the country from which the UE is roaming from. The P-CSCF determines the country to which the UE is belonging to based on the content of the P-Asserted-Identity header field which contains the home network domain name in a SIP URI belonging to the user; and
- the country of roaming partners, if the request originates from a different country then the country of the network to which the P-CSCF belongs to. Access technology specific procedures are described in each access technology specific annex to determine from which country and roaming partner the request was originated. If the country from which the request originates can not be determined all lists are associated.

If the P-CSCF detects that the Request-URI of the initial request for a dialog, or a standalone transaction, or an unknown method matches one of the emergency service identifiers in the associated lists, the P-CSCF shall:

- 0A) determine the geographical location of the UE. Access technology specific procedures are described in each access technology specific annex:
  - a) if the UE is roaming and the P-CSCF is in the home operator's network, or the SDP of the request describes CS media (see 3GPP TS 24.292 [80]), then the P-CSCF:
    - I) shall reject the request as specified in subclause 5.2.10.5;
  - b) if the UE is roaming and the P-CSCF is in the same network where the UE is roaming, or the UE is not roaming, then the P-CSCF, depending on operator policies:
    - I) may reject the request as specified in subclause 5.2.10.5; or
    - II) may continue with the next steps;

NOTE 1: Roaming is when a UE is in a geographic area that is outside the serving geographic area of the home IM CN subsystem.

NOTE 2: Emergency service URN in the request-URI indicates for the network that the emergency call attempt is recognized by the UE.

- 1) include in the Request-URI an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69], if necessary. If information on the type of emergency service is known include a sub-service type. The entry in the Request-URI that the P-CSCF includes shall be:
  - if the received Request-URI matches an emergency service URN, as received from the UE in the Request-URI; and
  - if the received Request-URI does not match an emergency service URN, as deduced from the Request-URI received from the UE;



- 1A) if operator policy requires that emergency service requests are forwarded to the S-CSCF and the P-CSCF determines that the network to which the originating user is attached (see the IP-CAN specific annexes for the detailed procedure) is the network the P-CSCF is in then:
- a) execute the procedure described in subclause 5.2.6.3.3, subclause 5.2.6.3.7, subclause 5.2.6.3.11 and subclause 5.2.7.2, as appropriate except for routing to IBCF;
  - b) before the request is forwarded in the referenced procedures, include a bottom most Route header field set to the URI associated with an E-CSCF;

NOTE 3: It is implementation dependent as to how the P-CSCF obtains the list of E-CSCFs.

- 1B) if the condition for 1A) is not fulfilled then:
- a) execute the procedure described in subclause 5.2.6.3.3, subclause 5.2.6.3.7, subclause 5.2.6.3.11 and subclause 5.2.7.2, as appropriate except for verifying the preloaded route against the received Service-Route header field; and routing to IBCF;
  - b) before the request is forwarded in the referenced procedures, remove all Route header fields and include a Route header field set to the URI associated with an E-CSCF;

NOTE 4: It is implementation dependent as to how the P-CSCF obtains the list of E-CSCFs.

- 1C) if the request is from a UE that is not considered as privileged sender and if the alternative identity of the originator of the request was not identified (see subclause 5.2.6.3.1):
- i) if the P-Asserted-Identity header field in the request to be sent contains a SIP URI and if a tel URI belongs to the set of implicitly registered public user identities that contains the SIP URI, add a second P-Asserted-Identity header field that contains the first tel URI of the implicitly registered public user identities; and
  - ii) if the P-Asserted-Identity header field in the request to be sent contains a tel URI, add a second P-Asserted-Identity header field that contains the first SIP URI of the implicitly registered public user identities that contains the tel URI;
- 2) if the request contains a Contact header field containing a GRUU the P-CSCF shall save the GRUU received in the Contact header field of the request and associate it with the UE IP address and UE port such that the P-CSCF is able to route target refresh request containing that GRUU in the Request-URI. The UE port used for the association is determined as follows:
- if IMS AKA or SIP digest with TLS is being used as a security mechanism, the UE protected server port for the security association on which the request was received; or
  - if SIP digest without TLS is being used as a security mechanism, the UE unprotected port on which the request was received; and
- 3) where the network uses the Resource-Priority header field to control the priority of emergency calls, add a Resource-Priority header field containing a namespace of "esnet" as defined in RFC 7135 [197].

If the P-CSCF does not receive any response to the initial request for a dialog or standalone transaction or an unknown method sent to an E-CSCF (including its retransmissions); or receives a 480 (Temporarily Unavailable) response to an initial request for a dialog or standalone transaction or an unknown method sent to an E-CSCF, the P-CSCF shall include a URI, associated with a different E-CSCF that has not been tried before for this initial request for the dialog or standalone transaction (including its retransmissions), in the topmost Route header field and forward the request.

If the P-CSCF does not receive any response to the initial request for a dialog or standalone transaction or an unknown method sent to a S-CSCF (including its retransmissions); or receives a 480 (Temporarily Unavailable) response to an initial request for a dialog or standalone transaction or an unknown method sent to a S-CSCF, the P-CSCF shall include a URI, associated with a different E-CSCF that has not been tried before for this initial request for the dialog or standalone transaction (including its retransmissions), in the topmost Route header field of the initial request for a dialog or standalone transaction or an unknown method, and forward the request.

If the P-CSCF:

- does not receive any response to this initial request for a dialog or standalone transaction or an unknown method (including its retransmissions); or receives a 3xx response or 480 (Temporarily Unavailable) response to an initial request for a dialog or standalone transaction or an unknown method, and if all E-CSCFs have been tried

before for this initial request for the dialog or standalone transaction (including its retransmissions), the P-CSCF shall reject this request as specified in subclause 5.2.10.5;

- receives:

- 1) any 4xx response other than a 480 (Temporarily Unavailable) response;
- 2) any 5xx response;
- 3) any 6xx response,

and the entry in the Request-URI as received from the UE is not in accordance with RFC 5031 [69], then the P-CSCF shall reject this request as specified in subclause 5.2.10.5.

If the P-CSCF receives from the IP-CAN (e.g. via PCRF) an indication that the requested resources for the multimedia session being established cannot be granted and the entry in the Request-URI as received from the UE is not in accordance with RFC 5031 [69], then the P-CSCF shall:

- send a CANCEL request to cancel the request forwarded to the selected E-CSCF; and
- reject this request as specified in subclause 5.2.10.5.

When the P-CSCF received a subsequent request in the dialog from the UE, and the network uses the Resource-Priority header field to control the priority of emergency calls, the P-CSCF shall add a Resource-Priority header field containing a namespace of "esnet" as defined in RFC 7135 [197].

When the P-CSCF receives a target refresh request for a dialog with the Request-URI containing a GRUU the P-CSCF shall:

- obtain the UE IP address and UE port associated to the GRUU contained in the Request-URI and rewrite the Request-URI with that UE IP address and UE port; and
- perform the steps in subclause 5.2.6.4 for when the P-CSCF receives, destined for the UE, a target refresh request for a dialog.

### 5.2.10.5 Abnormal and rejection cases

If the IM CN subsystem to where the P-CSCF belongs to is not capable to handle emergency sessions or due to local policy does not handle emergency sessions or only handles certain type of emergency session request or does not support emergency sessions for either the geographical location of the UE is located or the IP-CAN to which the UE is attached, or the SDP of the request describes CS media (see 3GPP TS 24.292 [80]), or for reasons described in subclause 5.2.10.4, the P-CSCF shall not forward the initial request for a dialog or standalone transaction or an unknown method. The P-CSCF:

I) shall reject the request by returning a 380 (Alternative Service) response;

II) if:

- support for the 3GPP IM CN subsystem XML body as described in subclause 7.6 in the Accept header field is not indicated, the P-CSCF shall assume that the UE supports version 1 of the 3GPP XML Schema for the IM CN subsystem XML; or
- if both the "sv" and "schemaversion" parameters are present, then the P-CSCF shall ignore the value of the "schemaversion" parameter;

III) shall include in the 380 (Alternative Service) response:

- a Content-Type header field with the value set to associated MIME type of the 3GPP IM CN subsystem XML body as described in subclause 7.6.1;
- a P-Asserted-Identity header field set to the value of the SIP URI of the P-CSCF included in the Path header field during the registration of the user whose UE sent the request causing this response (see subclause 5.2.2.1); and
- if the type of emergency service can be deduced from the Request-URI received from the UE, a Contact header field with an emergency service URN, i.e. a service URN with a top-level service type of "sos" as

specified in RFC 5031 [69], including sub-service type deduced from the Request-URI received from the UE;  
and

IV) shall include an IM CN subsystem XML body with the following elements:

- a) an <ims-3gpp> element with the "version" attribute set to "1" and with an <alternative-service> child element, set to the parameters of the alternative service;
  - i) a <type> child element, set to "emergency" (see table 7.6.2) to indicate that it was an emergency call;
  - ii) a <reason> child element, set to an operator configurable reason; and
  - iii) an <action> child element, set to "emergency-registration" (see table 7.6.3) if the P-CSCF is accordingly configured by the operator.

NOTE 1: Emergency service URN in the request-URI indicates for the network that the emergency call attempt is recognized by the UE.

NOTE 2: Some networks only allow session requests with a Request-URI containing an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69].

## 5.2.11 Void

# 5.3 Procedures at the I-CSCF

## 5.3.1 Registration procedure

### 5.3.1.1 General

During the registration procedure the I-CSCF shall behave as a stateful proxy.

### 5.3.1.2 Normal procedures

When the I-CSCF receives a REGISTER request, the I-CSCF shall verify whether or not it has arrived from a trusted domain. If the request has not arrived from a trusted domain, the I-CSCF shall complete the processing of the request by responding with 403 (Forbidden) response. Otherwise, the I-CSCF starts the user registration status query procedure to the HSS as specified in 3GPP TS 29.228 [14].

NOTE 1: The I-CSCF can find out whether the request arrived from a trusted domain or not, from the procedures described in 3GPP TS 33.210 [19A].

NOTE 2: Different UEs, each with its own private user identity, can register the same shared public user identity. Registrations of all public user identities belonging to these UEs are directed to the same S-CSCF as described in 3GPP TS 29.228 [14].

If the REGISTER request does not include an Authorization header field and private user identity, the I-CSCF shall derive the private user identity from the public user identity being registered, contained in the To header field, by removing URI scheme and the following parts of the URI if present: port number, URI parameters, and To header field parameters.

Prior to performing the user registration query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14]. As a result of the query the I-CSCF gets the Redirect-Host AVP.

If the user registration status query response from the HSS includes a valid SIP URI, the I-CSCF shall:

- 1) replace the Request-URI of the received REGISTER request with the SIP URI received from the HSS in the Server-Name AVP;
- 2) optionally include the received Redirect-Host AVP value in the P-User-Database header field as defined in RFC 4457 [82]; and
- 3) forward the REGISTER request to the indicated S-CSCF.

NOTE 3: The P-User-Database header field can be included only if the I-CSCF can assume (e.g. based on local configuration) that the receiving S-CSCF will be able to process the header field.

If the user registration status query response from the HSS includes a list of capabilities, the I-CSCF shall:

- 1) select a S-CSCF that fulfils the indicated mandatory capabilities – if more than one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;
- 2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;
- 3) optionally, include the received Redirect-Host AVP value in the P-User-Database header field as defined in RFC 4457 [82]; and
- 4) forward the REGISTER request to the selected S-CSCF.

NOTE 4: The P-User-Database header field can be included only if the I-CSCF can assume (e.g. based on local configuration) that the receiving S-CSCF will be able to process the header field.

NOTE 5: It is important that the I-CSCF does not alter the Via header field for requests and responses sent in the direction from the UE to the S-CSCF in the case of GPRS-IMS-Bundled authentication

When the I-CSCF receives a 2xx response to a REGISTER request, the I-CSCF shall forward the 2xx response to the P-CSCF.

### 5.3.1.3 Abnormal cases

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 403 (Forbidden) response to the UE.

If the HSS sends a negative response to the user registration status query request, the I-CSCF shall send back a 403 (Forbidden) response.

If the user registration status query procedure cannot be completed, e.g. due to time-out or incorrect information from the HSS, the I-CSCF shall send back a 480 (Temporarily Unavailable) response to the UE.

If a selected S-CSCF:

- does not respond to the REGISTER request and its retransmissions by the I-CSCF; or
- sends back a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request;

and:

- the REGISTER request did not include an "integrity-protected" header field parameter in the Authorization header field;
- the REGISTER request did include an "integrity-protected" header field parameter in the Authorization header field with a value set to "no" in the Authorization header field;
- the REGISTER request did include an "integrity-protected" header field parameter in the Authorization header field with a value set to other than "no" and the I-CSCF supports S-CSCF restoration procedures; or
- the REGISTER request did not include an Authorization header field and the I-CSCF supports S-CSCF restoration procedures;

then:

- if the I-CSCF has received the list of capabilities from the HSS, the I-CSCF shall select a new S-CSCF as described in subclause 5.3.1.2, based on the capabilities indicated from the HSS. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same registration procedure; or
- if the I-CSCF has received a valid SIP URI from the HSS because the S-CSCF is already assigned to other UEs sharing the same public user identity, it will request the list of capabilities from the HSS and, on receiving these capabilities, the I-CSCF shall select a new S-CSCF as described in subclause 5.3.1.2, based on the capabilities indicated from the HSS. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same registration procedure.

NOTE 1: Checking for the inclusion of the Authorization header field is necessary to prevent S-CSCF reselection in the case of GPRS-IMS-Bundled authentication or NASS-IMS bundled authentication when no Authorization header field is present in case I-CSCF does not support S-CSCF restoration procedures.

NOTE 2: In case the S-CSCF does not respond, the I-CSCF can apply a pre-configured timer based on local policy before re-selecting a new S-CSCF.

If a selected S-CSCF does not respond to a REGISTER request and its retransmissions by the I-CSCF and none of the conditions specified above in this case are fulfilled, the I-CSCF shall send back a 504 (Server Time-Out) response to the user, in accordance with the procedures in RFC 3261 [26].

If the I-CSCF cannot select a S-CSCF which fulfils the mandatory capabilities indicated by the HSS, the I-CSCF shall send back a 600 (Busy Everywhere) response to the user.

## 5.3.2 Initial requests

### 5.3.2.1 Normal procedures

The I-CSCF may behave as a stateful proxy for initial requests.

Upon receipt of a request, the I-CSCF shall perform the originating procedures as described in subclause 5.3.2.1A if the topmost Route header field of the request contains the "orig" parameter. Otherwise, the I-CSCF shall continue with the rest of the procedures of this subclause.

When the I-CSCF receives a request, the I-CSCF shall verify whether it has arrived from a trusted domain or not. If the request has arrived from a non trusted domain, then the I-CSCF shall remove all P-Charging-Vector header fields and all P-Charging-Function-Addresses header fields the request may contain.

NOTE 1: The I-CSCF can find out whether the request arrived from a trusted domain or not, from the procedures described in 3GPP TS 33.210 [19A].

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the I-CSCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs.

NOTE 2: The special treatment can include filtering, higher priority processing, routing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

The I-CSCF shall discard the P-Profile-Key header field, if the I-CSCF receives the P-Profile-Key header field in a SIP request or response.

When the I-CSCF receives, destined for a served user or a PSI, an initial request for a dialog or standalone transaction the I-CSCF shall:

- 1) if the Request-URI includes:
  - a) a pres: or an im: URI, then translate the pres: or im: URI to a public user identity and replace the Request-URI of the incoming request with that public user identity; or
  - b) a SIP-URI that is not a GRUU and with the user part starting with a + and the "user" SIP URI parameter equals "phone" then replace the Request-URI with a tel-URI with the user part of the SIP-URI in the telephone-subscriber element in the tel-URI, and carry forward the tel-URI parameters that may be present in the Request-URI; or
  - c) a SIP URI that is a GRUU, then obtain the public user identity or an identity of the UE that represents the functionality within the UE that performs the role of registrar from the Request-URI and use it for location query procedure to the HSS. When forwarding the request, the I-CSCF shall not modify the Request-URI of the incoming request;

NOTE 3: SRV records have to be advertised in DNS pointing to the I-CSCF for pres: and im: queries.

- 2) remove its own SIP URI from the topmost Route header field, if present; and
- 3) check if the domain name of the Request-URI matches with one of the PSI subdomains configured in the I-CSCF. If the match is successful, the I-CSCF resolves the Request-URI by an internal DNS mechanism into the IP address of the AS hosting the PSI and does not start the user location query procedure. Otherwise, the I-CSCF will start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [14] for the called PSI or user, indicated in or derived from the Request-URI. Prior to performing the user location query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

When the I-CSCF receives any response to such a request, the I-CSCF shall store the value of the "term-ioi" header field parameter received in the P-Charging-Vector header field, if present.

NOTE 4: A received "term-ioi" header field parameter will be a type 3 IOI. The type 3 IOI if received from an AS hosting a PSI or a type 2 IOI if received from the S-CSCF of the served user identifies the service provider from which the response was sent and the type 2 IOI identifies the network from which the response was sent.

When the I-CSCF receives an INVITE request, the I-CSCF may require the periodic refreshment of the session to avoid hung states in the I-CSCF. If the I-CSCF requires the session to be refreshed, then the I-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 5: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

In case the I-CSCF is able to resolve the Request-URI into the IP address of the AS hosting the PSI, then the I-CSCF shall:

- 1) store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field and retain the "icid-value" header field parameter in the P-Charging-Vector header field. If no "icid-value" header field parameter was found, then create a new, globally unique value for the "icid-value" header field parameter and insert it into the P-Charging-Vector header field. The I-CSCF shall insert a type 3 "orig-ioi" header field parameter in place of any received "orig-ioi" header field parameter. The I-CSCF shall set the type 3 "orig-ioi" header field parameter to a value that identifies the sending network of the request. The I-CSCF shall not include the type 3 "term-ioi" header field parameter; and
- 2) forward the request directly to the AS hosting the PSI.

Upon successful user location query, when the response contains the URI of the assigned S-CSCF, or the URI of an AS hosting the PSI, the I-CSCF shall:

- 1) insert the URI received from the HSS as the topmost Route header field;
- 2) store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field and retain the "icid-value" header field parameter in the P-Charging-Vector header field. If no "icid-value" header field parameter was found, then create a new, globally unique value for the "icid-value" header field parameter and insert it into the P-Charging-Vector header field;
- 3) optionally, include the received Redirect-Host AVP value in the P-User-Database header field as defined in RFC 4457 [82];
- 3A) if the Wildcarded Identity value is received from the HSS in the Wildcarded-Identity AVP and the I-CSCF supports the SIP P-Profile-Key private header extension, include the wildcarded identity value in the P-Profile-Key header field as defined in RFC 5002 [97]; and
- 4) forward the request based on the topmost Route header field.

NOTE 6: The P-User-Database header field can be included only if the I-CSCF can assume (e.g. based on local configuration) that the receiving S-CSCF will be able to process the header field.

Upon successful user location query, when the response contains information about the required S-CSCF capabilities, the I-CSCF shall:

- 1) if overlap signalling using the multiple-INVITEs method is supported as a network option, and if the I-CSCF receives an INVITE request outside an existing dialog with the same Call ID and From header as a previous

INVITE request during a certain period of time, route the new INVITE to the same next hop as the previous INVITE request; otherwise

- 2) select a S-CSCF according to the method described in 3GPP TS 29.228 [14];
- 3) insert the URI of the selected S-CSCF as the topmost Route header field value;
- 4) execute the procedure described in step 2 and 3 in the above paragraph (upon successful user location query, when the response contains the URI of the assigned S-CSCF);
- 5) optionally, include the received Redirect-Host AVP value in the P-User-Database header field as defined in RFC 4457 [82];
- 6) if the Wildcarded Identity value is received from the HSS in the Wildcarded-Identity AVP and the I-CSCF supports the the SIP P-Profile-Key private header extension, include the wildcarded identity value in the P-Profile-Key header field as defined in RFC 5002 [97]; and

NOTE 7: A Wildcarded Identity can be either a PSI or a public user identity.

- 7) forward the request to the selected S-CSCF.

NOTE 8: The P-User-Database header field can be included only if the I-CSCF can assume (e.g. based on local configuration) that the receiving S-CSCF will be able to process the header field.

Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, and if the Request-URI is a tel URI containing a public telecommunications number as specified in RFC 3966 [22], the I-CSCF may support a local configuration option that indicates whether or not request routing is to be attempted. If the local configuration option indicates that request routing is to be attempted, then the I-CSCF shall perform one of the following procedures based on local operator policy:

- 1) forward the request to the transit functionality for subsequent routing; or
- 2) invoke the portion of the transit functionality that translates the public telecommunications number contained in the Request-URI to a routeable SIP URI, and process the request based on the result, as follows:
  - a) if the translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g. a MRFC to play an announcement) in the home network, or the I-CSCF may send an appropriate SIP response to the originator, such as 404 (Not Found) or 604 (Does not exist anywhere). When forwarding the request to a BGCF or any other appropriate entity, the I-CSCF shall leave the original Request-URI containing the tel URI unmodified:
    - i) if overlap signalling using the multiple-INVITEs method is supported as a network option, and if the I-CSCF receives an INVITE request outside an existing dialog with the same Call ID and From header as a previous INVITE request during a certain period of time, the I-CSCF shall route the new INVITE to the same next hop as the previous INVITE request; and
    - ii) additional procedures apply if the I-CSCF supports NP capabilities and these capabilities are enabled by local policy, and the database used for translation from an international public telecommunications number to a SIP URI also provides NP data (for example, based on the PSTN Enumservice as defined by RFC 4769 [114] or other appropriate data bases). If the above translation from an international public telecommunications number to a SIP URI failed, but NP data was obtained from the database, then the I-CSCF shall update the tel-URI in the Request-URI with the obtained NP data, prior to forwarding the request to the BGCF or other appropriate entity. The URI is updated by the I-CSCF by adding the NP parameters defined by RFC 4694 [112] to the tel-URI in the Request-URI: an "npdi" tel-URI parameter is added to indicate that NP data retrieval has been performed, and if the number is ported, an "rn" tel-URI parameter is added to identify the ported-to routing number. The I-CSCF shall perform these procedures if the tel-URI in the received Request-URI does not contain an "npdi" tel-URI parameter. In addition, the I-CSCF may, based on local policy, perform these procedures when the tel-URI in the received Request-URI contains an "npdi" tel-URI parameter indicating that the NP data has been previously obtained; or

NOTE 9: The I-CSCF might need to update NP data added by a previous network if the previous network's NP database did not contain the local ported data for the called number.

- b) if this translation succeeds, then replace the Request-URI with the routeable SIP URI and process the request as follows:

- determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header field if present, otherwise based on the Request-URI. If the destination requires interconnect functionalities (e.g. the destination address is of an IP address type other than the IP address type used in the IM CN subsystem), the I-CSCF shall forward the request to the destination address via an IBCF in the same network;
- if network hiding is needed due to local policy, put the address of the IBCF to the topmost Route header field;
- route the request based on SIP routing procedures; and
- if overlap signalling using the multiple-INVITE method is supported as a network option, and if the I-CSCF receives an INVITE request outside an existing dialog with the same Call ID and From header as a previous INVITE request during a certain period of time, route the new INVITE to the same next hop as the previous INVITE request.

Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, and if local operator policy does not indicate that request routing is to be attempted, then, the I-CSCF shall return an appropriate unsuccessful SIP response. Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, and if the Request-URI is a SIP URI, the I-CSCF shall also return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) or 604 (Does not exist anywhere) in the case the user is not a user of the home network.

Upon an unsuccessful user location query when the response from the HSS indicates that the user is not registered and no services are provided for such a user, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) response if the user is recognized as a valid user, but is not registered at the moment and it does not have services for unregistered users.

When the I-CSCF receives an initial request for a dialog or standalone transaction, that contains a single Route header field pointing to itself, the I-CSCF shall determine from the entry in the Route header field whether it needs to do HSS query. In case HSS query not is needed, then the I-CSCF shall:

- 1) remove its own SIP URI from the topmost Route header field; and
- 2) route the request based on the Request-URI.

When the I-CSCF receives an initial request for a dialog or standalone transaction containing more than one Route header field, the I-CSCF shall:

- 1) remove its own SIP URI from the topmost Route header field; and
- 2) forward the request based on the topmost Route header field.

NOTE 10: In accordance with SIP the I-CSCF can add its own routeable SIP URI to the top of the Record-Route header field to any request, independently of whether it is an initial request. The P-CSCF will ignore any Record-Route header field that is not in the initial request of a dialog.

When the I-CSCF receives a response to an initial request (e.g. 183 (Session Progress) response or 2xx response), the I-CSCF shall store the values from the P-Charging-Function-Addresses header field, if present. If the next hop is outside of the current network, then the I-CSCF shall remove the P-Charging-Function-Addresses header field prior to forwarding the message.

When the I-CSCF, upon sending an initial INVITE request to the S-CSCF, receives a 305 (Use Proxy) response from the S-CSCF, the I-CSCF shall forward the initial INVITE request to the SIP URI indicated in the Contact field of the 305 (Use Proxy) response, as specified in RFC 3261 [26].

### 5.3.2.1A Originating procedures for requests containing the "orig" parameter

The procedures of this subclause apply for requests received at the I-CSCF when the topmost Route header field of the request contains the "orig" parameter.

The I-CSCF shall verify for all requests whether they arrived from a trusted domain or not. If the request arrived from a non trusted domain, then the I-CSCF shall respond with 403 (Forbidden) response.

If the request arrived from a trusted domain, the I-CSCF shall perform the procedures below.



NOTE 1: The I-CSCF can find out whether the request arrived from a trusted domain or not, from the procedures described in 3GPP TS 33.210 [19A].

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the I-CSCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs.

NOTE 2 The special treatment can include filtering, higher priority processing, routing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

If the I-CSCF receives the P-Profile-Key header field in a SIP request or response the I-CSCF shall discard the P-Profile-Key header field.

When the I-CSCF receives an initial request for a dialog or standalone transaction the I-CSCF will start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [14] for the calling user, indicated in either:

- 1) the P-Served-User header field, if included in the request; or
- 2) the P-Asserted-Identity header field, if the P-Served-User header field is not included in the request.

Prior to performing the user location query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

When the I-CSCF receives an INVITE request, the I-CSCF may require the periodic refreshment of the session to avoid hung states in the I-CSCF. If the I-CSCF requires the session to be refreshed, the I-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 3: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

When the response for user location query contains information about the required S-CSCF capabilities, the I-CSCF shall select a S-CSCF according to the method described in 3GPP TS 29.228 [14].

If the user location query was successful, the I-CSCF shall:

- 1) insert the URI of an AS hosting the PSI, or the URI of the S-CSCF - either received from the HSS, or selected by the I-CSCF based on capabilities - as the topmost Route header field appending the "orig" parameter to the URI of the S-CSCF;
- 2) store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field and retain the "icid-value" header field parameter in the P-Charging-Vector header field. If no "icid-value" header field parameter was found, then create a new, globally unique value for the "icid-value" header field parameter and insert it into the P-Charging-Vector header field;
- 3) optionally, include the received Redirect-Host AVP value in the P-User-Database header field as defined in draft-camarillo-sipping-user-database [82];
- 4) if a wildcarded identity value is received from the HSS in the Wildcarded-Identity AVP and the I-CSCF supports the SIP P-Profile-Key private header extension, include the wildcarded public user identity value in the P-Profile-Key header field as defined in RFC 5002 [97]; and
- 5) forward the request based on the topmost Route header field.

NOTE 4: The P-User-Database header field can be included only if the I-CSCF can assume (e.g. based on local configuration) that the receiving S-CSCF will be able to process the header field.

Upon an unsuccessful user location query, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) response or 604 (Does not exist anywhere) response in the case the user is not a user of the home network.

When the I-CSCF receives any response to the above request, and forwards it to AS, the I-CSCF shall:

- store the values from the P-Charging-Function-Addresses header field, if present. If the next hop is outside of the current network, then the I-CSCF shall remove the P-Charging-Function-Addresses header field prior to forwarding the message; and
- insert a P-Charging-Vector header field containing the type 3 "orig-ioi" header field parameter, if received in the request, and a type 3 "term-ioi" header field parameter in the response. The I-CSCF shall set the type 3 "term-ioi" header field parameter to a value that identifies the sending network of the response and the type 3 "orig-ioi" header field parameter is set to the previously received value of type 3 "orig-ioi" header field parameter.

### 5.3.2.2 Abnormal cases

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 404 (Not Found) response to the UE.

Upon successful user location query, when the response contains the URI of the assigned S-CSCF, if the I-CSCF is unable to contact the assigned S-CSCF, as determined by one of the following:

- the S-CSCF does not respond to the service request and its retransmissions by the I-CSCF; or
- by unspecified means available to the I-CSCF;

and:

- the I-CSCF supports S-CSCF restoration procedures;

then:

- the I-CSCF shall explicitly request the list of capabilities from the HSS and, on receiving these capabilities, the I-CSCF shall select a new S-CSCF, based on the capabilities indicated from the HSS. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same terminating procedure. Re-selection shall be performed until SIP transaction timer expires as specified in RFC 3261 [26].

NOTE 1: These procedures do not prevent the usage of unspecified reliability or recovery techniques above and beyond those specified in this subclause.

Upon successful user location query, when the response contains information about the required S-CSCF capabilities, if the I-CSCF is unable to contact a selected S-CSCF, as determined by one of the following:

- the S-CSCF does not respond to the service request and its retransmissions by the I-CSCF; or
- by unspecified means available to the I-CSCF;

then:

- the I-CSCF shall select a new S-CSCF, based on the capabilities indicated from the HSS. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same terminating procedure. Re-selection shall be performed until SIP transaction timer expires as specified in RFC 3261 [26].

NOTE 2: These procedures do not prevent the usage of unspecified reliability or recovery techniques above and beyond those specified in this subclause.

If the I-CSCF receives a negative response to the user location query, the I-CSCF shall send back a 404 (Not Found) response.

If the I-CSCF receives a CANCEL request and if the I-CSCF finds an internal state indicating a pending Cx transaction with the HSS, the I-CSCF:

- shall answer the CANCEL request with a 200 (OK) response; and
- shall answer the original request with a 487 (Request Terminated) response.

NOTE 3: The I-CSCF will discard any later arriving (pending) Cx answer message from the HSS.

With the exception of 305 (Use Proxy) response, the I-CSCF may recurse on a 3xx response only when the domain part of the URI contained in the 3xx response is in the same domain as the I-CSCF. For the same cases, if the URI is an IP

address, the I-CSCF shall only recurse if the IP address is known locally to be a address that represents the same domain as the I-CSCF.

### 5.3.3 Void

#### 5.3.3.1 Void

#### 5.3.3.2 Void

#### 5.3.3.3 Void

### 5.3.4 Void

## 5.4 Procedures at the S-CSCF

### 5.4.0 General

Where the S CSCF provides emergency call support, the procedures of subclause 5.4.8 shall be applied first.

### 5.4.1 Registration and authentication

#### 5.4.1.1 Introduction

The S-CSCF shall determine which authentication mechanism applies based on the contents of the REGISTER request and the authentication mechanism assigned in the HSS:

- 1) if the REGISTER request contains an Authorization header field with the "integrity-protected" header field parameter set to "no", the S-CSCF shall perform the initial registration procedures with IMS-AKA authentication described in subclauses 5.4.1.2.1 and 5.4.1.2.1A;
- 2) if the REGISTER request contains an Authorization header field with the "integrity-protected" header field parameter set to "yes", the S-CSCF shall perform the protected registration procedures with IMS-AKA as a security mechanism as described in subclause 5.4.1.2.2;
- 3) if the REGISTER request does not contain an Authorization header field, then the S-CSCF shall identify the user by the public user identity as received in the To header field of the REGISTER request. The S-CSCF shall derive the private user identity from the public user identity being registered. The S-CSCF shall derive the private user identity by removing SIP URI scheme and the following parts of the SIP URI if present: port number, URI parameters, and To header field parameters or by alternative mechanisms to derive the private user identity if operator policy requires to do so. These alternative mechanisms are not defined in this version of the specification;
- 4) if the REGISTER request does not contain an Authorization header field and the access type field in the P-Access-Network-Info header field indicated xDSL, Ethernet, or Fiber access, and containing the "network provided" header field parameter and the S-CSCF supports NASS-IMS-bundled authentication but does not support SIP digest, then the S-CSCF shall perform the initial registration procedures with NASS-IMS bundled authentication as a security mechanism as described in subclause 5.4.1.2.1D;
- 5) if the REGISTER request does not contain an Authorization header field and the access type field in the P-Access-Network-Info header field indicates it is received from an IPCAN different from 3GPP and containing the "network provided" header field parameter and the S-CSCF supports SIP digest but does not support NASS-IMS-bundled authentication, then the S-CSCF shall perform the initial registration procedures with SIP digest as a security mechanism as described in subclauses 5.4.1.2.1 and 5.4.1.2.1B;
- 6) if the REGISTER request does not contain an Authorization header field and there is no P-Access-Network-Info header field containing the "network provided" field or there is a P-Access-Network-Info header field indicating a 3GPP access network containing the "network provided", and the S-CSCF supports GPRS-IMS-Bundled authentication, the S-CSCF shall perform the initial registration procedures with GPRS-IMS-Bundled authentication described in subclause 5.4.1.2.1E;
- 7) if the REGISTER request does not contain an Authorization header field, and the P-Access-Network-Info header field indicates it is received from an access network other than 3GPP, xDSL, Ethernet or Fiber and containing the "network provided" header field parameter, and the S-CSCF supports SIP digest and NASS-IMS bundled

authentication, the S-CSCF shall perform the initial registration procedures with SIP digest as a security mechanism as described in subclauses 5.4.1.2.1 and 5.4.1.2.1B:

- 8) if the REGISTER request does not contain an Authorization header field, and the P-Access-Network-Info header field indicates it is received from a xDSL, Ethernet or Fiber access network, and containing the "network provided" header field parameter, and the S-CSCF supports SIP digest and NASS-IMS bundled authentication, the S-CSCF sends an authentication request for the user to the HSS indicating that the authentication scheme is unknown as described in 3GPP TS 29.228 [14]:
  - if the HSS responds with an authentication scheme of SIP digest, then the S-CSCF shall perform the initial registration procedures with SIPdigest as a security mechanism as described in subclauses 5.4.1.2.1 and 5.4.1.2.1B; or
  - if the HSS responds with an authentication scheme of NASS-IMS bundled authentication and the request was received from a P-CSCF in the home network and the P-CSCF is "TISpan-enabled", then the S-CSCF shall perform the initial registration procedures with NASS-IMS bundled authentication as a security mechanism as described in subclause 5.4.1.2.1D;
- 9) if the REGISTER request contains an Authorization header field without an "integrity-protected" header field parameter, the S-CSCF shall send an authentication request for the user to the HSS indicating that the authentication scheme is unknown as described in 3GPP TS 29.228 [14]:
  - if the HSS responds with an authentication scheme of NASS-IMS bundled authentication and the request was received from a P-CSCF is in the home network and the P-CSCF is "TISpan-enabled", then the S-CSCF shall perform the initial registration procedures with NASS-IMS bundled authentication as a security mechanism as described in subclause 5.4.1.2.1D; or
  - if the HSS responds with an authentication scheme of SIP digest, then the S-CSCF shall perform the initial registration procedures with SIPdigest as a security mechanism as described in subclauses 5.4.1.2.1 and 5.4.1.2.1B;
- 10) if the REGISTER request contains an Authorization header field with the "integrity-protected" header field parameter set to "tls-pending", "tls-yes", "ip-assoc-pending" or "ip-assoc-yes", the S-CSCF shall perform the protected registration procedures for SIP digest described in subclause 5.4.1.2.2A; and
- 11) if the REGISTER request contains an Authorization header field with the "integrity-protected" header field parameter set to "auth-done", the S-CSCF shall perform the protected registration procedures described in subclause 5.4.1.2.2E.

NOTE 1: The S-CSCF needs to be configured to know which P-CSCFs are "TISpan-enabled" and uses the Via header field to determine which P-CSCF forwarded the registration request.

The S-CSCF shall act as the SIP registrar for all UEs belonging to the IM CN subsystem and with public user identities.

Subclause 5.4.1.2 through subclause 5.4.1.7 define S-CSCF procedures for SIP registration that do not relate to emergency. All registration requests are first screened according to the procedures of subclause 5.4.8.2 to see if they do relate to an emergency registration.

For all SIP registrations identified:

- as relating to an emergency; or
- if priority is supported, as containing an authorised Resource-Priority header field;

the S-CSCF shall give priority over other registrations. This allows special treatment of such registrations.

NOTE 2: The special treatment can include filtering, higher priority processing, routing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

The S-CSCF shall support the use of the Path and Service-Route header field. The S-CSCF shall also support the Require and Supported header fields. The Path header field is only applicable to the REGISTER request and its 200 (OK) response. The Service-Route header field is only applicable to the 200 (OK) response of REGISTER. The S-CSCF shall not act as a redirect server for REGISTER requests.

The network operator defines minimum and maximum times for each registration. These values are provided within the S-CSCF.

The procedures for notification concerning automatically registered public user identities of a user are described in subclause 5.4.2.1.2.

In case a device performing address and/or port number conversions is provided by a NA(P)T or NA(P)T-PT, the S-CSCF may need to modify the SIP signalling according to the procedures described in annex K if both a "reg-id" and "+sip.instance" header field parameter are present in the received Contact header field as described in RFC 5626 [92].

## 5.4.1.2 Initial registration and user-initiated reregistration

### 5.4.1.2.1 Unprotected REGISTER

Any REGISTER request received unprotected by the S-CSCF without an Authorization header field, or with an Authorization header field having the "integrity-protected" header field parameter in the Authorization header field set to "no", or without an "integrity-protected" header field parameter is considered to be an initial registration. If such an initial registration contains a private user identity specifically reserved for IM CN subsystem registrations from an MSC Server enhanced for ICS as defined in 3GPP TS 23.003 [3], the S-CSCF shall respond with a 403 (Forbidden) response. The S-CSCF shall consider this registration attempt as failed..

NOTE 1: For NASS-IMS bundled authentication and GPRS-IMS-Bundled Authentication there is no distinction between a protected and an unprotected REGISTER. There is only an unprotected REGISTER to consider.

NOTE 2: If IMS AKA or SIP digest with TLS are used as a security mechanism, a 200 (OK) final response to an initial registration will only be sent back after the S-CSCF receives a correct authentication challenge response in a REGISTER request that is sent integrity protected.

NOTE 3: A REGISTER with the registration expiration interval value equal to zero will always be received protected. However, it is possible that in error conditions a REGISTER with the registration expiration interval value equal to zero can be received unprotected. In that instance the procedures below will be applied.

Upon receipt of a REGISTER request that is part of an initial registration as outlined above, for a public user identity for which the maximum number of allowed simultaneously registration flows for the used UE (i.e. linked to the same private user identity and instance ID) is reached, if the REGISTER is adding a new registration flow, then the S-CSCF shall reject the REGISTER by generating a 403 (Forbidden) response. If not, the S-CSCF shall continue with the rest of the procedures of this subclause.

Upon receipt of a REGISTER request that is part of an initial registration as outlined above, for a user identity linked to a private user identity and instance ID/reg-id if available, that has previously registered one or more public user identities, the S-CSCF shall:

- 1) perform the procedure below in this subclause for receipt of a REGISTER request for a public user identity which is not already registered, for the received public user identity;
- 2) if the multiple registrations is not used and if the authentication that in step 1) has been successful, and there are public user identities (including the public user identity being registered, if previously registered) that belong to this user that have been previously registered with the same private user identity, and with an old contact address different from the one received in the REGISTER request, and the previous registrations have not expired, perform the network initiated deregistration procedure (as described in subclause 5.4.1.5) for the previously registered public user identities belonging to this user including the public user identity being registered, if previously registered; and
- 3) if the multiple registrations is used (i.e., the "reg-id" header field parameter is included in the REGISTER request), and if the authentication that concludes the initial registration has been successful, and if the public user identity being registered has been previously registered with the same private user identity and the same "+sip.instance" and "reg-id" header field parameter values, and the previous registration has not expired:
  - a) identify the registration flow being replaced;
  - b) terminate any dialog, as specified in subclause 5.4.5.1.2, with a status code 480 (Temporarily Unavailable) in the Reason header field of the BYE request, associated with the registration flow being replaced; and

- c) send a NOTIFY request to the subscribers to the registration event package for the public user identity indicated in the REGISTER request, as described in subclause 5.4.2.1.2.

NOTE 4: The way the S-CSCF identifies the dialogs associated with the registration flow being replaced is implementation specific.

NOTE 5: The S-CSCF will inform the HSS that the previously registered public user identities, excluding the public user identity being registered, have been deregistered.

NOTE 6: Contact related to emergency registration is not affected. S-CSCF is not able deregister contact related to emergency registration and will not delete that.

When S-CSCF receives a REGISTER request with the "integrity-protected" header field parameter in the Authorization header field set to "no" and a non-empty "response" Authorization header field parameter, the S-CSCF shall ignore the value of the "response" header field parameter.

Upon receipt of a REGISTER request that is part of an initial registration as outlined above, for a public user identity which is not already registered linked to the same private user identity and the "+sip.instance" and "reg-id" header field parameters, if available, the S-CSCF shall:

- 1) identify the user by the public user identity as received in the To header field and if the REGISTER request includes an Authorization header field, identify the private user identity as received in the "username" Authorization header field parameter of the REGISTER request;
- 2) check if the P-Visited-Network-ID header field is included in the REGISTER request, and if it is included identify the visited network by the value of this header field;
- 3) select an authentication vector for the user. If no authentication vector for this user is available, after the S-CSCF has performed the Authentication procedure with the HSS, as described in 3GPP TS 29.228 [14], the S-CSCF shall select an authentication vector as described in 3GPP TS 33.203 [19].

Prior to performing Authentication procedure with the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14] or use the value as received in the P-User-Database header field in the REGISTER request as defined in RFC 4457 [82];

NOTE 7: The HSS address received in the response to SLF query or as a value of P-User-Database header field can be used to address the HSS of the public user identity in further queries.

NOTE 8: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be used by the HSS to direct all subsequent incoming initial requests for a dialog or standalone transactions destined for this user to this S-CSCF.

NOTE 9: When passing its SIP URI to the HSS, the S-CSCF may include in its SIP URI the transport protocol and the port number where it wants to be contacted.

- 4) store the "icid-value" header field parameter received in the P-Charging-Vector header field;
- 5) challenge the user by generating a 401 (Unauthorized) response for the received REGISTER request appropriate to the security mechanism in use;
- 6) send the so generated 401 (Unauthorized) response towards the UE, and if the URI in the first Path header field has an "ob" SIP URI parameter, include a Require header field with the option-tag "outbound" as described in RFC 5626 [92]; and
- 7) start timer reg-await-auth which guards the receipt of the next REGISTER request.

If the received REGISTER request indicates that the challenge sent previously by the S-CSCF to the UE was deemed to be invalid by the UE, the S-CSCF shall stop the timer reg-await-auth and proceed as described in the subclause 5.4.1.2.3.

#### 5.4.1.2.1A Challenge with IMS AKA as security mechanism

On sending a 401 (Unauthorized) response to an unprotected REGISTER request, the S-CSCF shall populate the header fields as follows:

- 1) a WWW-Authenticate header field which transports:
  - a globally unique name of the S-CSCF in the "realm" header field parameter;
  - the RAND and AUTN parameters and optional server specific data for the UE in the "nonce" header field parameter;
  - the security mechanism, which is "AKAv1-MD5", in the "algorithm" header field parameter;
  - the IK (Integrity Key) parameter for the P-CSCF in the "ik" header field parameter (see subclause 7.2A.1); and
  - the CK (Cipher Key) parameter for the P-CSCF in the "ck" header field parameter (see subclause 7.2A.1).

The S-CSCF shall store the RAND parameter used in the 401 (Unauthorized) response for future use in case of a resynchronisation. If a stored RAND already exists in the S-CSCF, the S-CSCF shall overwrite the stored RAND with the RAND used in the most recent 401 (Unauthorized) response.

#### 5.4.1.2.1B Challenge with SIP digest as security mechanism

On sending a 401 (Unauthorized) response to an unprotected REGISTER request, the S-CSCF shall populate the header fields as follows:

- 1) a WWW-Authenticate header field as defined in RFC 2617 [21], which transports:
  - a protection domain in the "realm" header field parameter;
  - a "nonce" header field parameter (generated by the S-CSCF);
  - an "algorithm" header field parameter; if the algorithm value is not provided in the authentication vector, it shall have the value "MD5"; and
  - a "qop" header field parameter; if the qop value is not provided in the authentication vector, it shall contain the value "auth".

#### 5.4.1.2.1C Challenge with SIP digest with TLS as security mechanism

The procedures for subclause 5.4.1.2.1B apply.

**NOTE:** The S-CSCF is not able to distinguish between SIP Digest with TLS and SIP Digest without TLS for the case of an unprotected REGISTER request, therefore the procedures are the same for both.

#### 5.4.1.2.1D Initial registration and user-initiated reregistration for NASS-IMS bundled authentication

Upon receipt of a REGISTER request that is determined to be NASS-IMS bundled authentication, for a user identity linked to a private user identity that has a registered public user identity but with a new contact address, the S-CSCF shall:

- 1) perform the procedure for receipt of a REGISTER request without the "integrity-protected" header field parameter in the Authorization header field or without the Authorization header field, for the received public user identity; and
- 2) if the Contact header field of the REGISTER request does not contain a "reg-id" header field parameter (i.e., the multiple registrations mechanism is not used), and the authentication has been successful, and there are public user identities (including the public user identity being registered, if previously registered) belonging to this user that have been previously registered with the same private user identity and with an old contact address different from the one received in the REGISTER request and if the previous registration have not expired:
  - a) terminate all dialogs, if any, associated with the previously registered public user identities (including the public user identity being registered, if previously registered), with a status code 480 (Temporarily Unavailable) in the Reason header field of the BYE request, as specified in subclause 5.4.5.1.2;
  - b) send a NOTIFY request, to the subscribers to the registration event package of the previously registered public user identities, that indicates that all previously registered public user identities (excluding the public user identity being registered) belonging to this user identified with its private user identity, have been

deregistered, as described in subclause 5.4.2.1.2. For the public user identity being registered, the NOTIFY request contains the new contact information; and

NOTE 1: The last dialog to be terminated will be the dialog established by the UE subscribing to the reg event package. When sending the NOTIFY request to the UE over this dialog, the S-CSCF will terminate this dialog by setting in the NOTIFY request the Subscription-State header field to the value of "terminated".

c) delete all information associated with the previously registered public user identities.

NOTE 2: Contact related to emergency registration is not affected. The S-CSCF is not able to deregister contact related to emergency registration and will not delete it.

Upon receipt of a REGISTER request that is determined to be NASS-IMS bundled authentication, for a public user identity for which the maximum number of allowed simultaneously registration flows is for the used UE (i.e. linked to the same private user identity and instance ID) is reached, if the REGISTER is adding a new registration flow, then the S-CSCF shall reject the REGISTER by generating a 403 (Forbidden) response. If not, the S-CSCF shall continue with the rest of the procedures of this subclause;

Upon receipt of a REGISTER request without the "integrity-protected" header field parameter in the Authorization header field or without an Authorization header field, which is not for an already registered public user identity linked to the same private user identity, the S-CSCF shall:

- 1) identify the user by the public user identity as received in the To header field of the REGISTER request and if the Authorization header field is present, the private user identity as received in the Authorization header field of the REGISTER request. If the Authorization header field is not present, the S-CSCF shall derive the private user identity from the public user identity being registered by removing SIP URI scheme and the following parts of the SIP URI if present: port number, URI parameters, and To header field parameters;
- 2) check whether one or more Line-Identifiers previously received over the Cx interface, and stored as a result of a Authentication procedure with the HSS, are available for the user. If not, the S-CSCF performs the Authentication procedure with the HSS, as described in 3GPP TS 29.228 [14], in order to obtain these Line-Identifiers;
- 3) in the particular case where the S-CSCF received via the Cx interface one or more Line-Identifiers, compare each of Line-Identifiers with the "dsl-location", "eth-location" or "fiber-location" parameter of the P-Access-Network-Info header field (if present and if it includes the "network-provided" parameter):
  - if one of these match, the user is considered authenticated, behave as described in step 5) to 11) of subclause 5.4.1.2.2;
  - otherwise i.e. if these do not match, return a 403 (Forbidden) response to the REGISTER request; and
- 4) if no Line-Identifier is received over the Cx interface, send a 500 (Server Internal Error) response to the REGISTER request.

Upon receipt of a REGISTER request without the "integrity-protected" header field parameter in the Authorization header field or without an Authorization header field, for an already registered public user identity linked to the same private user identity, and for existing contact information, the S-CSCF shall behave as described in subclause 5.4.1.2.2F.

#### 5.4.1.2.1E Initial registration and user-initiated reregistration for GPRS-IMS-Bundled authentication

Upon receipt of a REGISTER request without an Authorization header field, the S-CSCF shall:

- 1) identify the user by the public user identity as received in the To header field of the REGISTER request. The S-CSCF shall derive the private user identity from the public user identity being registered by removing URI scheme and the following parts of the URI if present: port number, URI parameters, and To header field parameters;
- 1A) if the maximum number of simultaneously registration flows allowed for the related public user identity for the used UE (i.e. linked to the same private user identity and instance ID) is reached, then the S-CSCF shall reject the REGISTER by generating a 403 (Forbidden) response. If not, the S-CSCF shall continue with the rest of the steps;



- 2) check if the P-Visited-Network-ID header field is included in the REGISTER request, and if it is included identify the visited network by the value of this header field;
- 3) check whether an IP address is stored for this UE. If no IP address (or prefix) is stored for the UE, query the HSS as described in 3GPP TS 29.228 [14] with the derived private user identity and the public user identity as input and store the received IP address (or prefix) of the UE; if the S-CSCF receives a prefix from the HSS, it will only check against prefixes otherwise it will check against the full IP address;

NOTE 1: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

- 4) check whether a "received" header field parameter exists in the Via header field provided by the UE. If a "received" header field parameter exists, the S-CSCF shall compare the IP address recorded in the "received" header field parameter against the UE's IP address stored during registration. In case of IPv6 stateless autoconfiguration, the S-CSCF shall compare the prefix of the IP address recorded in the "received" header field parameter against the UE's IP address prefix stored during registration. If no "received" header field parameter exists in the Via header field provided by the UE, then the S-CSCF shall compare IP address recorded in the "sent-by" parameter against the stored UE IP address. In case of IPv6 stateless autoconfiguration, S-CSCF shall compare the prefix of the IP address recorded in the "sent-by" parameter against the UE's IP address prefix stored during registration. In any case, if the stored IP address (or prefix) and the (prefix of the) IP address recorded in the Via header field provided by the UE do not match, the S-CSCF shall query the HSS as described in 3GPP TS 29.228 [14] with the derived private user identity and the public user identity as input and store the received IP address (or prefix) of the UE. If the stored IP address (or prefix) and the (prefix of the) IP address recorded in the Via header field provided by the UE still do not match the S-CSCF shall reject the registration with a 403 (Forbidden) response and skip the following steps;
- 5) after performing the S-CSCF Registration/deregistration notification procedure with the HSS, as described in 3GPP TS 29.228 [14], store the following information in the local data:
  - a) the list of public user identities, including the registered own public user identity and its associated set of implicitly registered public user identities and wildcarded public user identities due to the received REGISTER request. Each public user identity is identified as either barred or non-barred;
  - b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria (the initial Filter Criteria for the Registered and common parts is stored and the unregistered part is retained for possible use later - in the case the S-CSCF is retained if the user becomes unregistered); and
  - c) if S-CSCF restoration procedures are supported, the restoration information if received as specified in 3GPP TS 29.228 [14];

NOTE 2: There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same implicit registration set belong to different service profiles.

- 6) update registration bindings as follows:
  - a) bind to each non-barred registered public user identity all registered contact information including all header field parameters contained in the Contact header field and all associated URI parameters with the exception of the "pub-gruu" and "temp-gruu" header field parameters as specified in RFC 5627 [93], and store information for future use; and
  - b) if the Contact URI in the Contact header field does not contain a "bnc" URI parameter, then for each binding that contains a "+sip.instance" Contact header field parameter, assign a new temporary GRUU, as specified in subclause 5.4.7A.3;

NOTE 3: There might be more than one contact information available for one public user identity.

NOTE 4: The barred public user identities are not bound to the contact information.

- 7) check whether a Path header field was included in the REGISTER request and construct a list of preloaded Route header fields from the list of entries in the received Path header field. The S-CSCF shall preserve the order of the preloaded Route header fields and bind them either to the contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used) and the contact information that was received in the REGISTER request;

NOTE 5: If this registration is a reregistration or an initial registration (i.e., there are previously registered public user identities belonging to the user that have not been deregistered or expired), then a list of pre-loaded Route header fields will already exist. If multiple registration mechanism was not used, then the existing list of pre-loaded Route header fields is bound to a respective contact address of the UE. However, if multiple registration mechanism was used, then the existing list of pre-loaded Route header fields is bound to a registration flow and the associated contact address that was used to send the REGISTER request. In either case, the new list replaces the old list.

- 8) determine the duration of the registration by checking the registration expiration interval value in the received REGISTER request and bind it either to the respective contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used). The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;
- 9) store the "icid-value" header field parameter received in the P-Charging-Vector header field; and
- 10) create and send a 200 (OK) response for the REGISTER request as specified in subclause 5.4.1.2.2F.

When a user de-registers, or is de-registered by the HSS, the S-CSCF shall delete the IP address stored for the UE.

#### 5.4.1.2.2 Protected REGISTER with IMS AKA as a security mechanism

Upon receipt of a REGISTER request with the "integrity-protected" header field parameter in the Authorization header field set to "yes", the S-CSCF shall identify the user by the public user identity as received in the To header field and the private user identity as received in the Authorization header field of the REGISTER request, and:

If the maximum number of simultaneously registration flows allowed for the related public user identity for the used UE (i.e. linked to the same private user identity and instance ID) is reached, then the S-CSCF shall reject the REGISTER by generating a 403 (Forbidden) response. If not, the S-CSCF shall continue with rest of the procedures of this subclause;

In the case that there is no authentication currently ongoing for this user (i.e. no timer reg-await-auth is running):

- 1) check if the user needs to be reauthenticated.

The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for REGISTER requests received without the "integrity-protected" header field parameter in the Authorization header field set to "yes".

If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the unprotected REGISTER in subclause 5.4.1.2.1, beginning with step 3). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph; and

- 2) check whether a registration expiration interval value is included in the REGISTER request and its value. If the registration expiration interval value indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the registration expiration interval value does not indicate zero, the S-CSCF:
  - if the REGISTER request does not contain a "reg-id" header field parameter and the contact address indicated in the Contact header field was not previously registered, send a 403 (Forbidden) response to the UE; and

NOTE 1: New contact address is always registered via an initial registration.

- 3) check whether the public user identity received in the To header field is already registered. If it is not registered, the S-CSCF shall proceed beginning with step 4B below. Otherwise, the S-CSCF shall:
  - send a 439 (First Hop Lacks Outbound Support) response to the UE, if the REGISTER request contains the "reg-id" Contact header field parameter and the "outbound" option tag in a Supported header field, but the first URI in the Path header field does not have an "ob" URI parameter; or
  - otherwise proceed beginning with step 6 below.

In the case that a timer reg-await-auth is running for this user the S-CSCF shall:

- 1) check if the Call-ID of the request matches with the Call-ID of the 401 (Unauthorized) response which carried the last challenge. The S-CSCF shall only proceed further if the Call-IDs match;

- 2) stop timer reg-await-auth;
- 3) check whether an Authorization header field is included, containing:
  - a) the private user identity of the user in the "username" header field parameter;
  - b) the algorithm which is "AKAv1-MD5" in the "algorithm" header field parameter; and
  - c) the authentication challenge response needed for the authentication procedure in the "response" header field parameter.

The S-CSCF shall only proceed with the following steps in this paragraph if the authentication challenge response was included;

- 4) check whether the received authentication challenge response and the expected authentication challenge response (calculated by the S-CSCF using XRES and other parameters as described in RFC 3310 [49]) match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if the challenge response received from the UE and the expected response calculated by the S-CSCF match;
- 4A) if the Contact header field of the REGISTER request does not contain a "reg-id" header field parameter (i.e., the multiple registrations mechanism is not used), and there are public user identities (including the public user identity being registered, if previously registered) that belong to this user that have been previously registered with the same private user identity, and with an old contact address different from the one received in the REGISTER request and if the previous registrations have not expired:
  - a) terminate all dialogs, associated with the previously registered public user identities (including the public user identity being registered, if previously registered), with a status code 480 (Temporarily Unavailable) in the Reason header field of the BYE request, as specified in subclause 5.4.5.1.2;
  - b) send a NOTIFY request, to the subscribers to the registration event package of the previously registered public user identities, that indicates that all previously registered public user identities (excluding the public user identity being registered) belonging to this user identified with its private user identity, have been deregistered, as described in subclause 5.4.2.1.2. For the public user identity being registered, the NOTIFY request contains the new contact information; and

NOTE 2: The last dialog to be terminated will be the dialog established by the UE subscribing to the reg event package. When sending the NOTIFY request to the UE over this dialog, the S-CSCF will terminate this dialog by setting in the NOTIFY request the Subscription-State header field to the value of "terminated".

- c) delete all information associated with the previously registered public user identities;

NOTE 3: Contact related to emergency registration is not affected. The S-CSCF is not able to deregister contact related to emergency registration and will not delete it.

- 4B) if the REGISTER request contains the "reg-id" Contact header field parameter and the "outbound" option tag in a Supported header field, but the first URI in the Path header field does not have an "ob" URI parameter, send a 439 (First Hop Lacks Outbound Support) response to the UE;
- 5) after performing the S-CSCF Registration/deregistration notification procedure with the HSS, as described in 3GPP TS 29.228 [14], store the following information in the local data:
  - a) the list of public user identities, including the registered own public user identity and its associated set of implicitly registered public user identities and wildcarded public user identities due to the received REGISTER request. Each public user identity is identified as either barred or non-barred;
  - b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria (the initial Filter Criteria for the Registered and common parts is stored and the unregistered part is retained for possible use later - in the case of the S-CSCF is retained if the user becomes unregistered); and
  - c) if S-CSCF restoration procedures are supported, the restoration information if received as specified in 3GPP TS 29.228 [14];

NOTE 4: There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same implicit registration set belong to different service profiles.

6) update registration bindings:

- a) if the Contact URI in the Contact header field does not contain a "bnc" URI parameter, then bind to each non-barred registered public user identity all registered contact information including all header field parameters contained in the Contact header field and all associated SIP URI parameters, with the exception of the "pub-gruu" and "temp-gruu" header field parameters as specified in RFC 5627 [93], and store information for future use;
- b) if the Contact URI in the Contact header field contains a "bnc" URI parameter, as a network option bind each non-barred registered public user identity to a contact address generated according to the procedures of RFC 6140 [191].

NOTE 5: It is assumed that when the Contact header field contains a "bnc" parameter, the associated public user identities obtained from the HSS are all of a form compatible with registration procedures as specified in RFC 6140 [191]; i.e. the set consists only of distinct public user identities containing global numbers in the international format or wildcarded public user identities representing multiple global numbers in the international format. The S-CSCF procedures for handling the error case where an associated public user identity is incompatible with RFC 6140 [191] is out of scope of this specification.

- c) if the Contact URI in the Contact header field does not contain a "bnc" URI parameter, then for each binding that contains a "+sip.instance" Contact header field parameter, assign a new temporary GRUU, as specified in subclause 5.4.7A.3;
- d) if the Contact header field of the REGISTER request contained a "+sip.instance" and a "reg-id" header field parameter, and the SIP URI in the Path header field inserted by the P-CSCF contained an "ob" SIP URI parameter header field, and:
  - if the public user identity has not previously been registered with the same "+sip.instance" and "reg-id" Contact header field parameter values, then create the registration flow in addition to any existing registration flow; or
  - if the public user identity has previously been registered with the same "+sip.instance" and "reg-id" header field parameter values, then determine whether the request refreshes or replaces an existing registration flow. If the request:
    - i) refreshes an existing registration flow, then the S-CSCF shall leave the flow intact; or
    - ii) replaces the existing registration flow with a new flow, then the S-CSCF shall:
      - a) terminate any dialog, as specified in subclause 5.4.5.1.2, with a status code 480 (Temporarily Unavailable) in the Reason header field of the BYE request, associated with the registration flow being replaced; and
      - b) send a NOTIFY request to the subscribers to the registration event package for the public user identity indicated in the REGISTER request, as described in subclause 5.4.2.1.2;

NOTE 6: The S-CSCF determines whether this REGISTER request replaces or refreshes an existing registration flow by examining the SIP URI in the Path header field inserted into the request by the P-CSCF (see subclause 5.2.2.1).

NOTE 7: The way the S-CSCF identifies the dialogs associated with the registration flow being replaced is implementation specific.

NOTE 8: There might be more than one contact information available for one public user identity.

NOTE 9: The barred public user identities are not bound to the contact information.

NOTE 10: Contact related to emergency registration is not affected. S-CSCF is not able to deregister contact related to emergency registration and will not delete that.

- 7) check whether a Path header field was included in the REGISTER request and construct a list of preloaded Route header fields from the list of entries in the received Path header field. The S-CSCF shall preserve the order of the preloaded Route header fields and bind them either to the contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used) and the contact information that was received in the REGISTER request;

NOTE 11: If this registration is a reregistration or an initial registration (i.e., there are previously registered public user identities belonging to the user that have not been deregistered or expired), then a list of pre-loaded Route header fields will already exist. If multiple registration mechanism was not used, then the existing list of pre-loaded Route header fields is bound to a respective contact address of the UE. However, if multiple registration mechanism was used, then the existing list of pre-loaded Route header fields is bound to a registration flow and the associated contact address that was used to send the REGISTER request. In either case, the new list replaces the old list.

- 8) determine the duration of the registration by checking the value of the registration expiration interval value in the received REGISTER request and bind it either to the respective contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used). The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;
- 9) store the "icid-value" header field parameter received in the P-Charging-Vector header field;
- 10) if an "orig-ioi" header field parameter is received in the P-Charging-Vector header field, store the value of the received "orig-ioi" header field parameter; and

NOTE 12: Any received "orig-ioi" header field parameter will be a type 1 IOI. The type 1 IOI identifies the network from which the request was sent.

- 11) create and send a 200 (OK) response for the REGISTER request as specified in subclause 5.4.1.2.2F.

#### 5.4.1.2.2A Protected REGISTER with SIP digest as a security mechanism

Upon receipt of a REGISTER request with the "integrity-protected" header field parameter in the Authorization header field set to "tls-pending", "tls=yes", "ip-assoc-pending", or "ip-assoc=yes", the S-CSCF shall identify the user by the public user identity as received in the To header field and the private user identity as received in the Authorization header field of the REGISTER request, and:

NOTE: Although the REGISTER request with the "integrity-protected" header field parameter set to "ip-assoc-pending" or "ip-assoc=yes" is handled as protected REGISTER request, the integrity of the request is actually not protected by SIP digest.

If the maximum number of simultaneously registration flows allowed for the related public user identity for the used UE (i.e. linked to the same private user identity and instance ID) is reached, then the S-CSCF shall reject the REGISTER by generating a 403 (Forbidden) response. If not, the S-CSCF shall continue with rest of the procedures of this subclause;

In the case that there is no authentication currently ongoing for this user (i.e. no timer reg-await-auth is running):

- 1) check if the user needs to be reauthenticated. The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for REGISTER requests received without the "integrity-protected" header field parameter in the Authorization header field set to "tls=yes".

If the user needs to be reauthenticated and the REGISTER did not include an Authorization header field with a digest response, the S-CSCF shall proceed with the authentication procedures as described for the initial REGISTER in subclause 5.4.1.2.1 and subclause 5.4.1.2.1B.

If the user needs to be reauthenticated and the REGISTER included an Authorization header field with a digest response, the S-CSCF shall proceed with the authentication procedures as described for the initial REGISTER in subclause 5.4.1.2.1 and subclause 5.4.1.2.1B and include the "stale" header field parameter with value "true" in the WWW-Authenticate header field.

In the case that a timer reg-await-auth is running for this user the S-CSCF shall:

- 1) check if the Call-ID of the request matches with the Call-ID of the 401 (Unauthorized) response which carried the last challenge. The S-CSCF shall only proceed further if the Call-IDs match;
- 2) stop timer reg-await-auth;
- 3) in the case the algorithm is "MD5", check the following additional fields:
  - a "realm" header field parameter matching the "realm" header field parameter in the authentication challenge;

- an "algorithm" header field parameter which matches the "algorithm" header field parameter sent in the authentication challenge;
- "nonce" header field parameter matching the "nonce" header field parameter in the authentication challenge;
- a "cnonce" header field parameter; and
- a nonce-count field.

The S-CSCF shall only proceed with the following steps in this paragraph if the authentication challenge response was included;

- 4) check whether the received authentication challenge response and the expected authentication challenge response match. The expected response is calculated by the S-CSCF as described in RFC 2617 [21] using the H(A1) value provided by the HSS. If the received authentication challenge response and the expected authentication challenge response match, then the UE is considered authenticated. If the UE is considered authenticated, and if the "integrity-protected" header field parameter in the Authorization header field is set to the value "tls-pending" or "tls-yes", then the S-CSCF shall associate the registration with the local state of "tls-protected";

NOTE 1: The S-CSCF can have a local security policy to treat messages other than initial REGISTER requests, messages relating to emergency services, and error messages, differently depending on whether the registration is associated with the state "tls-protected".

- 4A) if the REGISTER request contains the "reg-id" Contact header field parameter and the "outbound" option tag in a Supported header field, but the first URI in the Path header does not have an "ob" URI parameter, send a 439 (First Hop Lacks Outbound Support) response to the UE;
- 5) after performing the S-CSCF Registration/deregistration notification procedure with the HSS, as described in 3GPP TS 29.228 [14], store the following information in the local data:
  - a) the list of public user identities, including the registered own public user identity and its associated set of implicitly registered public user identities and wildcarded public user identities due to the received REGISTER request. Each public user identity is identified as either barred or non-barred;
  - b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria (the initial Filter Criteria for the Registered and common parts is stored and the unregistered part is retained for possible use later - in the case of the S-CSCF is retained if the user becomes unregistered); and
  - c) if S-CSCF restoration procedures are supported, the restoration information, if received, as specified in 3GPP TS 29.228 [14];

NOTE 2: There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same implicit registration set belong to different service profiles.

- 6) update registration bindings:
  - a) if the Contact URI in the Contact header field does not contain a "bnc" URI parameter, then bind to each non-barred registered public user identity all registered contact information including all header field parameters contained in the Contact header field and all associated URI parameters, with the exception of the "pub-gruu" and "temp-gruu" header field parameters as specified in RFC 5627 [93], and store information for future use;
  - b) if the Contact URI in the Contact header field contains a "bnc" URI parameter, as a network option bind each non-barred registered public user identity to a contact address as specified in RFC 6140 [191].

NOTE 3: It is assumed that when the Contact header field contains a "bnc" parameter, the associated public user identities obtained from the HSS are all of a form compatible with registration procedures as specified in RFC 6140 [191]; i.e. the set consists only of distinct public user identities containing global numbers in the international format or wildcarded public user identities representing multiple global numbers in the international format. The S-CSCF procedures for handling the error case where an associated public user identity is incompatible with RFC 6140 [191] is out of scope of this specification.

- c) if the Contact URI in the Contact header field does not contain a "bnc" URI parameter, then for each binding that contains a "+sip.instance" Contact header field parameter, assign a new temporary GRUU, as specified in subclause 5.4.7A.3;
- d) if the Contact header field of the REGISTER request does not contain a "reg-id" header field parameter (i.e., the multiple registrations mechanism is not used), and there are public user identities (including the public user identity being registered, if previously registered) that belong to this user that have been previously registered with the same private user identity, and with an old contact address different from the one received in the REGISTER request and if the previous registrations have not expired:
  - terminate all dialogs, associated with the previously registered public user identities (including the public user identity being registered, if previously registered), with a status code 480 (Temporarily Unavailable) in the Reason header field of the BYE request, as specified in subclause 5.4.5.1.2;
  - send a NOTIFY request, to the subscribers to the registration event package of the previously registered public user identities, that indicates that all previously registered public user identities (excluding the public user identity being registered) belonging to this user identified with its private user identity, have been deregistered, as described in subclause 5.4.2.1.2. For the public user identity being registered, the NOTIFY request contains the new contact information; and

NOTE 4: The last dialog to be terminated will be the dialog established by the UE subscribing to the reg event package. When sending the NOTIFY request to the UE over this dialog, the S-CSCF will terminate this dialog by setting in the NOTIFY request the Subscription-State header field to the value of "terminated".

- delete all information associated with the previously registered public user identities; and

NOTE 5: Contact related to emergency registration is not affected. The S-CSCF is not able to deregister contact related to emergency registration and will not delete it.

- e) if the Contact header field of the REGISTER request contained a "+sip.instance" and a "reg-id" header field parameter, and the SIP URI in the Path header field inserted by the P-CSCF contained an "ob" SIP URI parameter header field, and:
  - if the public user identity has not previously been registered with the same "+sip.instance" and "reg-id" Contact header field parameter values, then create the registration flow in addition to any existing registration flow; or
  - if the public user identity has previously been registered with the same "+sip.instance" and "reg-id" header field parameter values, then determine whether the request refreshes or replaces an existing registration flow. If the request:
    - i) refreshes an existing registration flow, then the S-CSCF shall leave the flow intact; or
    - ii) replaces the existing registration flow with a new flow, then the S-CSCF shall:
      - a) terminate any dialog, as specified in subclause 5.4.5.1.2, with a status code 480 (Temporarily Unavailable) in the Reason header field of the BYE request, associated with the registration flow being replaced; and
      - b) send a NOTIFY request to the subscribers to the registration event package for the public user identity indicated in the REGISTER request, as described in subclause 5.4.2.1.2;

NOTE 6: The S-CSCF determines whether this REGISTER request replaces or refreshes an existing registration flow by examining the SIP URI in the Path header field inserted into the request by the P-CSCF (see subclause 5.2.2.1).

NOTE 7: The way the S-CSCF identifies the dialogs associated with the registration flow being replaced is implementation specific.

NOTE 8: There might be more than one contact information available for one public user identity.

NOTE 9: The barred public user identities are not bound to the contact information.

NOTE 10: Contact related to emergency registration is not affected. S-CSCF is not able deregister contact related to emergency registration and will not delete that.

- 7) check whether a Path header field was included in the REGISTER request and construct a list of preloaded Route header fields from the list of entries in the received Path header field. The S-CSCF shall preserve the order of the preloaded Route header fields and bind them to either the the contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used) and contact information that was received in the REGISTER request;

NOTE 11: If this registration is a reregistration or an initial registration (i.e., there are previously registered public user identities belonging to the user that have not been deregistered or expired), then a list of pre-loaded Route header fields will already exist. If multiple registration mechanism was not used, then the existing list of pre-loaded Route header fields is bound to a respective contact address of the UE. However, if multiple registration mechanism was used, then the existing list of pre-loaded Route header fields is bound to a registration flow and the associated contact address that was used to send the REGISTER request. In either case, the new list replaces the old list.

- 8) determine the duration of the registration by checking the value of the registration expiration interval value in the received REGISTER request and bind it either to the respective contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used). The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;

- 9) store the "icid-value" header field parameter received in the P-Charging-Vector header field;

- 10) if an "orig-ioi" header field parameter is received in the P-Charging-Vector header field, store the value of the received "orig-ioi" header field parameter; and

NOTE 12: Any received "orig-ioi" header field parameter will be a type 1 IOI. The type 1 IOI identifies the network from which the request was sent.

- 11) create and send a 200 (OK) response for the REGISTER request as specified in subclause 5.4.1.2.2F. The S-CSCF shall also store the nonce-count value in the received REGISTER request and include an Authentication-Info header field containing the fields described in RFC 2617 [21] as follows:

- a "nextnonce" header field parameter if the S-CSCF requires a new nonce for subsequent authentication responses from the UE;
- a "qop" header field parameter matching the "qop" Authorization header field parameter sent by the UE;
- a "rspauth" header field parameter with a response-digest calculated as described in RFC 2617 [21];
- a "cnonce" header field parameter value matching the cnonce in the Authorization header field sent by the UE; and
- a "nonce-count" header field parameter matching the "nonce-count" Authorization header field parameter sent by the UE.

#### 5.4.1.2.2B Protected REGISTER with SIP digest with TLS as a security mechanism

The procedures for subclause 5.4.1.2.2A apply.

#### 5.4.1.2.2C NASS-IMS bundled authentication as a security mechanism

There is no protected REGISTER when NASS-IMS bundled authentication is used as a security mechanism. The procedures of subclause 5.4.1.2.1D apply to all REGISTER requests.

#### 5.4.1.2.2D GPRS-IMS-Bundled authentication as a security mechanism

There is no protected REGISTER when GPRS-IMS-Bundled authentication is used as a security mechanism. The procedures of subclause 5.4.1.2.1E apply to all REGISTER requests.

#### 5.4.1.2.2E Protected REGISTER – Authentication already performed

The S-CSCF shall not perform authentication of the user for any REGISTER request with the "integrity-protected" header field parameter in the Authorization header set to "auth-done".



In this release of this document, when the registration procedure as specified in this subclause is performed, i.e., the REGISTER request contains the "integrity-protected" header field parameter in the Authorization header set to "auth-done", the S-CSCF shall not employ outbound registration as described in RFC 5626 [92].

Upon receipt of a REGISTER request with the "integrity-protected" header field parameter in the Authorization header set to "auth-done", the S-CSCF shall identify the user by the public user identity as received in the To header field and the private user identity as received in the Authorization header field of the REGISTER request.

In addition the S-CSCF shall check whether a registration expiration interval value is included in the REGISTER request and its value. If the registration expiration interval value indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the registration expiration interval value does not indicate zero, the S-CSCF shall:

- 1) if the REGISTER request contains the "reg-id" header field parameter in the Contact header field, respond with a 403 (Forbidden) response to the REGISTER request; and
- 2) if there are public user identities (including the public user identity being registered, if previously registered) that belong to this user that have been previously registered with the same private user identity, and with an old contact address different from the one received in the REGISTER request and if the previous registrations have not expired:
  - a) terminate all dialogs, associated with the previously registered public user identities (including the public user identity being registered, if previously registered), with a status code 480 (Temporarily Unavailable) in the Reason header field of the BYE request, as specified in subclause 5.4.5.1.2;
  - b) send a NOTIFY request, to the subscribers to the registration event package of the previously registered public user identities, that indicates that all previously registered public user identities (excluding the public user identity being registered) belonging to this user identified with its private user identity, have been deregistered, as described in subclause 5.4.2.1.2. For the public user identity being registered, the NOTIFY request contains the new contact information; and

NOTE 1: The last dialog to be terminated will be the dialog established by the user (identified with its private user identity) subscribing to its own reg event package using the old contact address. When sending the NOTIFY request over this dialog, the S-CSCF will terminate this dialog by setting in the NOTIFY request the Subscription-State header field to the value of "terminated".

- c) delete all information associated with the previously registered public user identities;

Subsequently, the S-CSCF shall check whether the public user identity received in the To header field is already registered. If it is not registered, the S-CSCF shall proceed beginning with step 1 below. Otherwise, the S-CSCF shall proceed beginning with step 2 below.

- 1) after performing the S-CSCF Registration/deregistration notification procedure with the HSS, as described in 3GPP TS 29.228 [14], store the following information in the local data:
  - a) the list of public user identities, including the registered own public user identity and its associated set of implicitly registered public user identities and wildcarded public user identities due to the received REGISTER request. Each public user identity is identified as either barred or non-barred; and,
  - b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria (the initial Filter Criteria for the Registered and common parts is stored and the unregistered part is retained for possible use later - in the case of the S-CSCF is retained if the user becomes unregistered);

NOTE 2: There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same implicit registration set belong to different service profiles.

- 2) update registration bindings:
  - a) if the Contact URI in the Contact header field does not contain a "bnc" URI parameter, then bind to each non-barred registered public user identity all registered contact information including all header parameters contained in the Contact header and all associated URI parameters, with the exception of the URI "pub-gruu" and "temp-gruu" parameters as specified in RFC 5627 [93], and store information for future use;

- b) if the Contact URI in the Contact header field contains a "bnc" URI parameter, as a network option bind each non-barred registered public user identity to a contact address as specified in RFC 6140 [191].

NOTE 3: It is assumed that when the Contact header field contains a "bnc" parameter, the associated public user identities obtained from the HSS are all of a form compatible with registration procedures as specified in RFC 6140 [191]; i.e. the set consists only of distinct public user identities contain global numbers in the international format or wildcarded public user identities representing multiple global numbers in the international format. The S-CSCF procedures for handling the error case where an associated public user identity is incompatible with RFC 6140 [191] is out of scope of this specification.

- c) if the Contact URI in the Contact header field does not contain a "bnc" URI parameter, then for each binding that contains a "+sip.instance" header field parameter, assign a new temporary GRUU, as specified in subclause 5.4.7A.3.

NOTE 4: There might be more than one contact information available for one public user identity.

NOTE 5: The barred public user identities are not bound to the contact information.

- 3) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the received Path header field. The S-CSCF shall preserve the order of the preloaded Route header fields and bind them to the contact information that was received in the REGISTER request;

NOTE 6: If this registration is a reregistration or an initial registration (i.e., there are previously registered public user identities belonging to the user that have not been deregistered or expired), then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

- 4) determine the duration of the registration by checking the value of the registration expiration interval value in the received REGISTER request. The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;
- 5) store the "icid-value" header field parameter received in the P-Charging-Vector header;
- 6) if an "orig-ioi" header field parameter is received in the P-Charging-Vector header, store the value of the received "orig-ioi" header field parameter; and

NOTE 7: Any received "orig-ioi" header field parameter will be a type 1 IOI. The type 1 IOI identifies the network from which the request was sent.

- 7) create and send a 200 (OK) response for the REGISTER request as specified in subclause 5.4.1.2.2F.

#### 5.4.1.2.2F Successful registration

If a 200 (OK) response is to be sent for a REGISTER request, the S-CSCF shall, in addition to any contents identified elsewhere in subclause 5.4.1.2, include:

- a) the list of received Path header fields;
- b) a P-Associated-URI header field containing the list of the registered distinct public user identity and its associated set of implicitly registered distinct public user identities. The first URI in the list of public user identities supplied by the HSS to the S-CSCF will indicate the default public user identity to be used by the S-CSCF. The public user identity indicated as the default public user identity must be a registered public user identity. The S-CSCF shall place the default public user identity as the first entry in the list of URIs present in the P-Associated-URI header field. The default public user identity will be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header field, as described in subclause 5.2.6.3. If the S-CSCF received a display name from the HSS for a public user identity, then the S-CSCF shall populate the P-Associated-URI header field entry for that public identity with the associated display name. The S-CSCF shall not add a barred public user identity to the list of URIs in the P-Associated-URI header field;

NOTE 1: The P-Associated-URI header field lists only the public user identity and its associated set of implicitly registered public user identities that have been registered, rather than the list of user's URIs that may be either registered or unregistered as specified in RFC 7315 [52]. If the registered public user identity which is not barred does not have any other associated public user identities or wildcarded public user identities, the P-Associated-URI header field lists only the registered public user identity itself, rather than an empty P-Associated-URI header field as specified in RFC 7315 [52]. The P-Associated-URI header field does not list wildcarded public user identities.

c) a Service-Route header field containing:

- the SIP URI identifying the S-CSCF containing an indication that subsequent requests routed via this service route (i.e. from the P-CSCF to the S-CSCF) was sent by the UE using either the contact address of the UE or the registration flow and the associated contact address (if the multiple registration mechanism is used) that has been registered and are treated as for the UE-originating case. This indication may e.g. be in a URI parameter, a character string in the user part of the URI or be a port number in the URI. The S-CSCF shall use a different SIP-URI for each registration. If the multiple registration mechanism is used, the S-CSCF shall also use a different SIP-URI for each registration flow associated with the registration; and
- if network topology hiding is required a SIP URI identifying an IBCF as the topmost entry;

NOTE 2: In accordance with the procedures described in RFC 3608 [38], an IBCF does not insert its own routable SIP URI to the Service-Route header field.

- d) a P-Charging-Function-Addresses header field containing the values received from the HSS if the P-CSCF is in the same network as the S-CSCF. It can be determined if the P-CSCF is in the same network as the S-CSCF by the contents of the P-Visited-Network-ID header field included in the REGISTER request;
- e) a P-Charging-Vector header field containing the "orig-ioi" header field parameter, if received in the REGISTER request and a type 1 "term-ioi" header field parameter. The S-CSCF shall set the type 1 "term-ioi" header field parameter to a value that identifies the sending network of the response and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter;
- f) a Contact header field listing all contact addresses for this public user identity, including all saved header field parameters and URI parameters (including all ICSI values and IARI values) received in the Contact header field of the REGISTER request;
- g) GRUUs in the Contact header field. If the REGISTER request contained a Required or Supported header field containing the value "gruu" then for each contact address in the Contact header field that has a "+sip.instance" header field parameter:
  - i) add "pub-gruu" header field parameter containing the public GRUU representing (as specified in subclause 5.4.7A.2) the association between the public user identity from the To header field in the REGISTER request and the instance ID contained in the "+sip.instance" header field parameter;
  - ii) if the Contact URI in the Contact header field does not contain a "bnc" URI parameter, then add a "temp-gruu" header field parameters. containing the most recently assigned temporary GRUU representing (as specified in subclause 5.4.7A) the association between the public user identity from the To header field in the REGISTER request and the instance ID contained in the "+sip.instance" header field parameter; and
  - iii) if the S-CSCF supports RFC 6140 [191] and the Contact URI in the Contact header field contains a "bnc" URI parameter, then add a "temp-gruu-cookie" header field parameter containing a value generated as specified in RFC 6140 [191]; and
- h) if the received REGISTER request contained both a "reg-id" and "+sip.instance" header field parameters in the Contact header field, and the first URI within the Path header field contains the "ob" SIP URI parameter a Require header field with the "outbound" option-tag as described in RFC 5626 [92];

NOTE 3: There might be other contact addresses available, that this UE or other UEs have registered for the same public user identity.

and send the so created 200 (OK) response to the UE.

For all service profiles in the implicit registration set, the S-CSCF shall send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria of the service profile from the HSS for the REGISTER event.

NOTE 4: If this registration is a reregistration, the Filter Criteria already exists in the local data.

NOTE 5: If the same AS matches the Filter Criteria of several service profiles for the event of REGISTER request, then the AS will receive several third-party REGISTER requests. Each of these requests will include a public user identity from the corresponding service profile.

The S-CSCF shall consider the public user identity being registered to be bound either to the contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used), as specified in the Contact header field, for the duration indicated in the registration expiration interval value.

#### 5.4.1.2.3 Abnormal cases - general

In the case that the expiration timer from the UE is too short to be accepted by the S-CSCF, the S-CSCF shall:

- reject the REGISTER request with a 423 (Interval Too Brief) response, containing a Min-Expires header field with the minimum registration time the S-CSCF will accept.

On receiving a failure response to one of the third-party REGISTER requests, based on the information in the Filter Criteria the S-CSCF may:

- abort sending third-party REGISTER requests; and
- initiate network-initiated deregistration procedure.

If the Filter Criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the AS, the S-CSCF shall not initiate network-initiated deregistration procedure.

In the case that the REGISTER request from the UE contains multiple SIP URIs which are different addresses as Contact header field entries, the S-CSCF shall store:

- the entry in the Contact header field with the highest value of the "q" header field parameter; or
- an entry decided by the S-CSCF based on local policy;

and include the stored entry in the 200 (OK) response.

In the case that the REGISTER request from the UE contains multiple SIP URIs which are the same addresses with the same value of the "q" Contact header field parameter, the S-CSCF shall not store multiple entries with the same "q" value but store one of the entries with the same "q" value based on local policy along with any entries that have different "q" values and include only the stored entries in the 200 (OK) response.

NOTE 1: The UE can register multiple SIP URIs in the Contact header field simultaneously, provided they all contain the same IP address and port number. In this case the S-CSCF behaviour is as defined RFC 3261 [26] (i.e multiple Contact header field entries are bound to the public user identity in the To header field and are returned in the 200 (OK) response).

NOTE 2: If the timer reg-await-auth expires, the S-CSCF will consider the authentication to have failed. If the public user identity was already registered, the S-CSCF will leave it registered, as described in 3GPP TS 33.203 [19].

For any error response, the S-CSCF shall insert a P-Charging-Vector header field containing the "orig-ioi" header field parameter, if received in the REGISTER request and a type 1 "term-ioi" header field parameter. The S-CSCF shall set the type 1 "term-ioi" header field parameter to a value that identifies the sending network of the response and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field.

NOTE 3: Any previously received "orig-ioi" header field parameter will be a type 1 IOI. The type 1 IOI identifies the visited network of the registered user.

If the Contact header field in the REGISTER request from the UE contains an invalid Contact URI as defined in RFC 6140 [191] (e.g., the Contact URI contains both a "bnc" and "user" URI parameter) then the S-CSCF shall reject the REGISTER request with a 400 (Bad Request) response.

#### 5.4.1.2.3A Abnormal cases – IMS AKA as security mechanism

In the case that the REGISTER request, that contains the authentication challenge response from the UE does not match with the expected REGISTER request (e.g. wrong Call-Id or authentication challenge response) and the request has the "integrity-protected" header field parameter in the Authorization header field set to "yes", the S-CSCF shall:

- send a 403 (Forbidden) response to the UE. The S-CSCF shall consider this authentication attempt as failed. The S-CSCF shall not update the registration state of the subscriber.

NOTE 1: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request, which was supposed to carry the response to the challenge, contains an empty "response" Authorization header field parameter (i.e. no authentication challenge response) and no "auts" Authorization header field parameters indicating that the MAC parameter was invalid in the challenge, the S-CSCF shall:

- respond with a 403 (Forbidden) response to the UE. The S-CSCF shall not update the registration state of the subscriber.

NOTE 2: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request from the UE containing an "auts" Authorization header field parameter, indicating that the SQN was deemed to be out of range by the UE, the S-CSCF will fetch new authentication vectors from the HSS. In order to indicate a resynchronisation, the S-CSCF shall include the value of the "auts" header field parameter received from the UE and the stored RAND, when fetching the new authentication vectors. On receipt of the new authentication vectors from the HSS, the S-CSCF shall either:

- send a 401 (Unauthorized) response to initiate a further authentication attempt, using these new vectors; or
- respond with a 403 (Forbidden) response if the authentication attempt is to be abandoned. The S-CSCF shall not update the registration state of the subscriber.

NOTE 3: If the UE was registered before, it stays registered until the registration expiration time expires.

NOTE 4: Since the UE responds only to two consecutive invalid challenges, the S-CSCF will send a 401 (Unauthorized) response that contains a new challenge only twice.

NOTE 5: In the case of an "auts" Authorization header field parameter being present in the REGISTER request, the "response" Authorization header field parameter in the same REGISTER request will not be taken into account by the S-CSCF.

In the case that the S-CSCF receives a REGISTER request with the "integrity-protected" header field parameter in the Authorization header field set to "yes", for which the public user identity received in the To header field and the private user identity received in the "username" Authorization header field parameter of the REGISTER request do not match to any registered user at this S-CSCF, if the S-CSCF supports S-CSCF restoration procedures, the S-CSCF shall behave as described in subclause 5.4.1.2.2, otherwise the S-CSCF shall:

- respond with a 500 (Server Internal Error) response to the UE.

NOTE 6: This error is not raised if there is a match on the private user identity, but no match on the public user identity.

#### 5.4.1.2.3B Abnormal cases – SIP digest as security mechanism

In the case that the REGISTER request, that contains the authentication challenge response from the UE does not match with the expected REGISTER request (e.g. wrong Call-Id or authentication challenge response) and the request has the "integrity-protected" header field parameter in the Authorization header field set to either "tls-pending", "tls-yes", "ip-assoc-pending", or "ip-assoc-yes", the S-CSCF shall do one of the following:

- send a 403 (Forbidden) response to the UE. The S-CSCF shall consider this authentication attempt as failed. The S-CSCF shall not update the registration state of the subscriber; or
- rechallenge the user by issuing a 401 (Unauthorized) response including a challenge as per the authentication procedures described in subclause 5.4.1.2.1B.

NOTE 1: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request from the UE contains an invalid "nonce" Authorization header field parameter with a valid challenge response for that nonce (indicating that the client knows the correct username/password), or when the nonce-count value sent by the UE is not the expected value, the S-CSCF shall:

- send a 401 (Unauthorized) response to initiate a further authentication attempt with a fresh nonce and the "stale" header field parameter set to "true" in the WWW-Authenticate header field.

In the case that the S-CSCF receives a REGISTER request with the "integrity-protected" header field parameter in the Authorization header field set to "tls-pending", "tls-yes", "ip-assoc-pending", or "ip-assoc-yes", for which the public user identity received in the To header field and the private user identity received in the Authorization header field of the REGISTER request do not match to any registered or initial registration pending user at this S-CSCF, if the S-CSCF supports S-CSCF restoration procedures, the S-CSCF shall behave as described in subclause 5.4.1.2.2A, otherwise the S-CSCF shall:

- respond with a 500 (Server Internal Error) response to the UE.

NOTE 2: This error is not raised if there is a match on the private user identity, but no match on the public user identity.

#### 5.4.1.2.3C Abnormal cases – SIP digest with TLS as security mechanism

The procedures for subclause 5.4.1.2.3B apply.

#### 5.4.1.2.3D Abnormal cases – NASS-IMS bundled authentication as security mechanism

There are no abnormal cases for NASS-IMS bundled authentication.

#### 5.4.1.2.3E Abnormal cases – GPRS-IMS-Bundled authentication as security mechanism

There are no abnormal cases for GPRS-IMS-Bundled authentication.

### 5.4.1.3 Authentication and reauthentication

Authentication and reauthentication is performed by the registration procedures as described in subclause 5.4.1.2.

#### 5.4.1.4 User-initiated deregistration

##### 5.4.1.4.1 Normal cases

When S-CSCF receives a REGISTER request with the registration expiration interval value containing the value zero, the S-CSCF shall:

- 1) verify that the REGISTER request is associated with an existing registered contact or an existing flow or, if the S-CSCF restoration procedures are supported by this S-CSCF, attempt to restore a contact or flow from HSS associated with the REGISTER request. If no associated contact or flow exists then the S-CSCF shall send a 481 (Call Leg/Transaction Does Not Exist) response to the UE and skip the remaining procedures in this subclause;
- 2) if IMS AKA is in use as the security mechanism, check whether the "integrity-protected" header field parameter in the Authorization header field set to "yes", indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps if the "integrity-protected" header field parameter is set to "yes";
- 3) if SIP digest without TLS or SIP digest with TLS is in use as a security mechanism, check whether the "integrity-protected" header field parameter in the Authorization header field set to "tls-yes" or "ip-assoc-yes", indicating that the REGISTER request was received from a previously registered user. If the "integrity-protected" header field parameter is set to "tls-pending", "ip-assoc-pending" or is not present the S-CSCF shall ensure authentication is performed as described in subclause 5.4.1.2.1 (and consequently subclause 5.4.1.2.1B or 5.4.1.2.1C) if local policy requires. The S-CSCF shall only proceed with the following steps if the "integrity-protected" header field parameter is set to "tls-yes", "ip-assoc-yes", or the required authentication is successfully performed if required by local policy;
- 4) if NASS-IMS bundled authentication is in use as a security mechanism, only proceed with the following steps if the "integrity-protected" header field parameter in the Authorization header field does not exist or without an Authorization header field, and one or more Line-Identifiers previously received over the Cx interface, stored as

a result of an Authentication procedure with the HSS, as described in 3GPP TS 29.228 [14], are available for the user;

- 4A) if the security mechanism as described in subclause 5.4.1.2.2E is in use, check whether the "integrity-protected" header field parameter in the Authorization header field set to "auth-done". The S-CSCF shall only proceed with the following steps if the "integrity-protected" header field parameter is set to "auth-done";
- 5) release all INVITE dialogs that include this user's contact addresses or the flows that are being deregistered, and where these dialogs were initiated by or terminated towards these contact addresses and the same public user identity found that was To header field that was received REGISTER request or with one of the implicitly registered public user identities by applying the steps listed in subclause 5.4.5.1.2;
- 6) examine the Contact header field in the REGISTER request, and:
  - a) if the value "\*" is not included in the Contact header field and:
    - i) if the "reg-id" header field parameter is not included in the Contact header field, then:
      - remove the binding (i.e. deregister) between the public user identity found in the To header field together with the implicitly registered public user identities and the contact addresses specified in the REGISTER request. The S-CSCF shall only remove the contact addresses that were registered by this UE;
    - ii) if the "reg-id" header field parameter and "+sip.instance" header field parameter are included in the Contact header field, and the UE supports multiple registrations (i.e. the "outbound" option tag is included in the Supported header field), then:
      - remove the binding (i.e. deregister) between the public user identity indicated in the To header field (together with the associated implicitly registered public user identities) and the flow identified by the "reg-id" header field parameter;
- 7) if the S-CSCF receives a REGISTER request with the value "\*" in the Contact header field and the value zero in the Expires header field, remove all contact addresses that were bound to the public user identity found in the To header field and have been registered by this UE identified with its private user identity;
- 8) for all service profiles in the implicit registration set send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria of the service profile from the HSS for the REGISTER event;
- 9) if this is a deregistration request for the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered) and there are still active multimedia sessions that includes this user's registered contact address, where the session was initiated by or terminated towards the contact with the registered contact address for that public user identity which is currently registered or with one of the implicitly registered public user identities, release only each of these multimedia sessions associated with the registered contact address by applying the steps listed in subclause 5.4.5.1.2. The S-CSCF shall only release dialogs associated to the multimedia sessions originated or terminated towards the registered user's contact address; and
- 10) send a 200 (OK) response to a REGISTER request that contains a list of Contact header fields enumerating all contacts and flows that are currently registered, and all contacts that have been deregistered. For each contact address and the flow that has been deregistered, the Contact header field shall contain the contact address and the "reg-id" header field parameter that identifies the flow, if a flow was deregistered, and the associated information, and the registration expiration interval value shall be set to zero.

If all public user identities of the UE are deregistered, then the S-CSCF may consider the UE and P-CSCF subscriptions to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header field containing a value of zero).

If the Authorization header field of the REGISTER request contained an "integrity-protected" header field parameter set to the value "no", the S-CSCF shall apply the procedures described in subclause 5.4.1.2.1.

On completion of the above procedures in this subclause and of the S-CSCF Registration/deregistration notification procedure with the HSS, as described in 3GPP TS 29.228 [14], for one or more public user identities, the S-CSCF shall update or remove those public user identities, their registration state and the associated service profiles from the local data. Based on operators' policy the S-CSCF can request the HSS to either be kept or cleared as the S-CSCF allocated to

this subscriber. If emergency contacts are still registered for this subscriber, the S-CSCF requests the HSS to be kept as the S-CSCF allocated to this subscriber.

#### 5.4.1.4.2 Abnormal cases - IMS AKA as security mechanism

If case that the S-CSCF receives a REGISTER request with the "integrity-protected" header field parameter in the Authorization header set to "yes", for which the public user identity received in the To header and the private user identity received in the Authorization header of the REGISTER request do not match to any registered user at this S-CSCF, if the S-CSCF supports S-CSCF restoration procedures as specified in 3GPP TS 23.380 [7D], the S-CSCF shall behave as described in subclause 5.4.1.4.1, otherwise the S-CSCF shall:

- respond with a 500 (Server Internal Error) response to the UE.

NOTE: This error is not raised if there is a match on the private user identity, but no match on the public user identity.

#### 5.4.1.4.4 Abnormal cases – SIP digest with TLS as security mechanism

The procedures for subclause 5.4.1.4.2 apply.

#### 5.4.1.4.5 Abnormal cases – NASS-IMS bundled authentication as security mechanism

There are no abnormal cases for NASS-IMS bundled authentication.

#### 5.4.1.4.6 Abnormal cases – GPRS-IMS-Bundled authentication as security mechanism

There are no abnormal cases for GPRS-IMS-Bundled authentication.

### 5.4.1.5 Network-initiated deregistration

NOTE 1: A network-initiated deregistration event that occurs at the S-CSCF can be received from the HSS or can be an internal event in the S-CSCF.

For any registered public user identity, the S-CSCF can deregister:

- all contact addresses bound to the indicated public user identity (i.e. deregister the respective public user identity);
- some contact addresses bound to the indicated public user identity;
- a particular contact address bound to the indicated public user identity; or
- one or more registration flows and the associated contact address bound to the indicated public user identity, when the UE supports multiple registration procedure;

by sending a single NOTIFY request.

Prior to initiating the network-initiated deregistration for the only currently registered public user identity and its associated set of implicitly registered public user identities and wildcarded public user identities that have been registered either with the same contact address of the UE or the same registration flow and the associated contact address (if the multiple registration mechanism is used), i.e. there are no other public user identities registered either with this contact address or with this registration flow and the associated contact address (if the multiple registration mechanism is used), and there are still active multimedia sessions belonging either to this contact address or to this registration flow and the associated contact address (if the multiple registration mechanism is used), the S-CSCF shall release only multimedia sessions belonging to this contact address or to this registration flow and the associated contact address (if the multiple registration mechanism is used) as described in the following paragraph. The multimedia sessions for the same public user identity, if registered either with another contact address or another registration flow and the associated contact address (if the multiple registration mechanism is used) remain unchanged.

Prior to initiating the network-initiated deregistration while there are still active multimedia sessions that are associated with this user and contact, the S-CSCF shall release none, some or all of these multimedia sessions by applying the steps listed in subclause 5.4.5.1.2 under the following conditions:

- when the S-CSCF does not expect the UE to reregister a given public user identity and its associated set of implicitly registered public user identities that have been registered with respective contact address (i.e. S-CSCF will set the event attribute within the respective <contact> element to "rejected" for the NOTIFY request, as



described below), the S-CSCF shall release all sessions that are associated with the registered contact address for the public user identities using the contact address that is being deregistered, which includes the implicitly registered public user identities.

- when the S-CSCF expects the UE to reregister a given public user identity and its associated set of implicitly registered public user identities that have been registered with respective contact address (i.e. S-CSCF will set the event attribute within the respective <contact> element to "deactivated" for the NOTIFY request, as described below), the S-CSCF shall only release sessions that currently include the user's contact address, where the session was initiated by or terminated towards the user with the contact address registered to one of the public user identities using the contact address that is being deregistered, which includes the implicitly registered public user identities.

When a network-initiated deregistration event occurs for one or more public user identities that are bound either to one or more contact addresses or registration flows and the associated contact addresses (if the multiple registration mechanism is used), the S-CSCF shall send a NOTIFY request to all subscribers that have subscribed to the respective reg event package. For each NOTIFY request, the S-CSCF shall:

- 1) set the Request-URI and Route header field to the saved route information during subscription;
- 2) set the Event header field to the "reg" value;
- 3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;
- 4) set the aor attribute within each <registration> element to one public user identity:
  - a) set the <uri> sub-element inside each <contact> sub-element of each <registration> element to the respective contact address provided by the UE;
  - b) if the public user identity:
    - i) has been deregistered (i.e. all contact addresses and all registration flows and associated contact addresses bound to the indicated public user identity are removed) then:
      - set the state attribute within the <registration> element to "terminated";
      - set the state attribute within each <contact> element belonging to this UE to "terminated"; and
      - set the event attribute within each <contact> element belonging to this UE to either "unregistered", or "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

NOTE 2: If the multiple registration mechanism is used, then the reg-id header field parameter will be included as an <unknown-param> element within each respective <contact> element.

NOTE 3: The UE will consider its public user identity as deregistered when the binding between the respective public user identity and all contact addresses and all registration flows and associated contact addresses (if the multiple registration mechanism is used) belonging to the UE have been removed.

- ii) has been kept registered then:
  - I) set the state attribute within the <registration> element to "active";
  - II) set the state attribute within each <contact> element to:
    - for the binding between the public user identity and either the contact address or a registration flow and associated contact addresses (if the multiple registration mechanism is used) to be removed set the state attribute within the <contact> element to "terminated", and event attribute element to either "unregistered", or "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or
    - for the binding between the public user identity and either the contact address or the registration flow and associated contact addresses (if the multiple registration mechanism is used) which remain unchanged, if any, leave the <contact> element unmodified, and if the contact has been assigned GRUUs and the Contact URI did not contain a "bnc" SIP URI parameter then set the <pub-gruu> and <temp-gruu> sub-elements of the <contact> element as specified in

RFC 5628 [94] and include the <unknown-param> sub-element within each <contact> to any additional header field parameters contained in the Contact header field of the REGISTER request according to RFC 3680 [43]; and

NOTE 4: There might be more than one contact information available for one public user identity. When deregistering this UE, the S-CSCF will only modify the <contact> elements that were originally registered by this UE using its private user identity. The <contact> elements of the same public user identity, if registered by another UE using different private user identities remain unchanged.

- 5) add a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

When sending a final NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities have been deregistered or expired), the S-CSCF shall also terminate the subscription to the registration event package by setting the Subscription-State header field to the value of "terminated".

Also, for all service profiles in the implicit registration set the S-CSCF shall send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria of the service profile from the HSS as if a equivalent REGISTER request had been received from the user deregistering that public user identity, or combination of public user identities.

On completion of the above procedures for one or more public user identities linked to the same private user identity, the S-CSCF shall consider those public user identities and the associated implicitly registered public user identities which have no contact address or a registration flow and associated contact addresses (if the multiple registration mechanism is used) bound to them as deregistered. On completion of the S-CSCF Registration/deregistration notification procedure with the HSS, as described in 3GPP TS 29.228 [14], the S-CSCF shall update or remove those public user identities linked to the same private user identity, their registration state and the associated service profiles from the local data (based on operators' policy the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber). On the completion of the Network initiated de-registration by the HSS procedure, as described in 3GPP TS 29.228 [14], the S-CSCF shall remove those public user identities, their registration state and the associated service profiles from the local data.

#### 5.4.1.6 Network-initiated reauthentication

The S-CSCF may request a subscriber to reauthenticate at any time, based on a number of possible operator settable triggers.

NOTE 1: Triggers for re-authentication include e.g. a current registration of the UE is set to expire at a predetermined time; one or more error conditions in the S-CSCF; the S-CSCF mistrusts the UE.

If the S-CSCF is informed that a private user identity needs to be re-authenticated, the S-CSCF shall generate a NOTIFY request on all dialogs which have been established due to subscription to the reg event package of that user. For each NOTIFY request the S-CSCF shall:

- 1) set the Request-URI and Route header field to the saved route information during subscription;
- 2) set the Event header field to the "reg" value;
- 3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns:
  - a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE;
  - b) set the aor attribute within each <registration> element to one public user identity;
  - c) set the state attribute within each <registration> element to "active";
  - d) set the state attribute within each <contact> element to "active";
  - e) set the event attribute within each <contact> element that was registered by this UE to "shortened";
  - f) set the expiry attribute within each <contact> element that was registered by this UE to an operator defined value; and

- g) if the Contact URI did not contain a "bnc" SIP URI parameter then set the <pub-gruu> and <temp-gruu> sub-elements within each <contact> element as specified in subclause 5.4.2.1.2; and

NOTE 2: There might be more than one contact information available for one public user identity. The S-CSCF will only modify the <contact> elements that were originally registered by this UE using its private user identity. The S-CSCF will not modify the <contact> elements for the same public user identity, if registered by another UE using different private user identity.

- 4) set a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17].

Afterwards the S-CSCF shall wait for the user to reauthenticate (see subclause 5.4.1.2).

NOTE 3: Network initiated re-authentication can occur due to internal processing within the S-CSCF.

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

When generating the NOTIFY request, the S-CSCF shall shorten the validity of all registration lifetimes associated with this private user identity to an operator defined value that will allow the user to be re-authenticated.

#### 5.4.1.7 Notification of Application Servers about registration status

During registration, the S-CSCF shall include the P-Access-Network-Info header fields (as received in the REGISTER request from the UE and the P-CSCF) and a P-Visited-Network-ID header field (as received in the REGISTER request from the UE) in the 3rd-party REGISTER request sent towards the ASs, if the AS is part of the trust domain. If the AS is not part of the trust domain, the S-CSCF shall not include any P-Access-Network-Info header field or P-Visited-Network-ID header field. The S-CSCF shall not include a P-Access-Network-Info header field in any responses to the REGISTER request.

If the registration procedure described in subclauses 5.4.1.2, 5.4.1.4 or 5.4.1.5 (as appropriate) was successful, the S-CSCF shall send a third-party REGISTER request to each AS with the following information:

- a) the Request-URI, which shall contain the AS's SIP URI;
- b) the From header field, which shall contain the S-CSCF's SIP URI;
- c) the To header field, which shall contain a non-barred public user identity belonging to the service profile of the processed Filter Criteria. It may be either a public user identity as contained in the REGISTER request received from the UE or one of the implicitly registered public user identities in the service profile, as configured by the operator;

NOTE 1: For the whole implicit registration set only one public user identity per service profile appears in the third-party REGISTER requests. Thus, based on third-party REGISTER requests only, the ASs will not have complete information on the registration state of each public user identity in the implicit registration set. The only way to have a complete and continuously updated information (even upon administrative change in subscriber's profile) is to subscribe to the reg event package.

- d) the Contact header field, which shall contain the S-CSCF's SIP URI;
- e) for initial registration and user-initiated reregistration (subclause 5.4.1.2), the registration expiration interval value, which shall contain the same value that the S-CSCF returned in the 200 (OK) response for the REGISTER request received from the UE;
- f) for user-initiated deregistration (subclause 5.4.1.4) and network-initiated deregistration (subclause 5.4.1.5), the registration expiration interval value, which shall contain the value zero;
- g) for initial registration and user-initiated reregistration (subclause 5.4.1.2), a message body, if there is Filter Criteria indicating the need to include HSS provided data for the REGISTER event (e.g. HSS may provide AS specific data to be included in the third-party REGISTER) or if there is Filter Criteria indicating the need to include the contents of the incoming REGISTER request or the contents of the 200 (OK) response to the incoming REGISTER request in the body of the third-party REGISTER. The S-CSCF shall format the MIME body and set the value of the Content-Type header field to include the MIME type specified in subclause 5.4.1.7A;

NOTE 2: When the AS is outside the trust domain for any header field that is permitted in the REGISTER request received from the UE or final response to the REGISTER request received from the UE, including an Include Register Request or Include Register Response indication in the initial Filter Criteria would cause the incoming REGISTER request or 200 (OK) response to the incoming REGISTER request contents to be delivered to the AS revealing information that AS is not trusted to obtain. Include Register Request and Include Register Response indication is therefore not included in the initial Filter Criteria for an AS that exists outside the trust domain for any such header field.

- h) for initial registration and user-initiated reregistration, the P-Charging-Vector header field, which shall contain the same "icid-value" header field parameter that the S-CSCF received in the REGISTER request from the UE. The S-CSCF shall insert a type 3 orig-ioi parameter in place of any received "orig-ioi" header field parameter and shall set the type 3 "orig-ioi" header field parameter to a value that identifies the sending network of the request. The S-CSCF shall not include the type 3 "term-ioi" header field parameter;
- i) for initial registration and user-initiated reregistration, a P-Charging-Function-Addresses header field, which shall contain the values received from the HSS if the message is forwarded within the S-CSCF home network; and
- j) in case the received REGISTER request contained a P-User-Database header field and the AS belongs to the same operator as the S-CSCF, optionally a P-User-Database header field which shall contain the received value.

When the S-CSCF receives any response to a third-party REGISTER request, the S-CSCF shall store the value of the "term-ioi" header field parameter received in the P-Charging-Vector header field, if present.

NOTE 3: Any received "term-ioi" header field parameter will be a type 3 IOI. The type 3 IOI identifies the service provider from which the response was sent.

If the S-CSCF fails to receive a SIP response or receives a 408 (Request Timeout) response or a 5xx response to a third-party REGISTER, the S-CSCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION\_CONTINUED" as specified in 3GPP TS 29.228 [14] or no default handling is indicated, no further action is needed; and
- if the default handling defined in the filter criteria indicates the value "SESSION\_TERMINATED" as specified in 3GPP TS 29.228 [14], initiate the network-initiated deregistration as described in subclause 5.4.1.5 for the currently registered public user identity and its associated set of implicitly registered non-barred public user identities bound to the contact(s) registered in the REGISTER request causing the third-party REGISTER request.

#### 5.4.1.7A Including contents in the body of the third-party REGISTER request

If there is a service information XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [14]), then in the third-party REGISTER request the S-CSCF shall:

- include in the message body the service information within the <service-info> XML which is a child XML element of an <ims-3gpp> element with the "version" attribute set to "1" element as described in subclause 7.6; and
- set the value of the content type to the MIME type specified in subclause 7.6.

If there is an Include Register Request XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [14]), then in the third-party REGISTER request the S-CSCF shall:

- include in the message body the incoming SIP REGISTER request within a "message/sip" MIME body as defined in RFC 3261 [26]; and
- set the value of the content type to "message/sip".

If there is an Include Register Response XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [14]), then in the third-party REGISTER request, the S-CSCF shall:

- include in the message body the 200 (OK) response to the incoming SIP REGISTER request within a "message/sip" MIME body as defined in RFC 3261 [26]; and
- set the value of the content type to "message/sip".

If there is more than one message body to be included in the third-party REGISTER request then in the third-party REGISTER request the S-CSCF shall:

- include a multipart message body and set the value of the Content-Type header field to "multipart/mixed" as specified in RFC 2046 [149] and RFC 5621 [150]; and
- set the Content-Type of the elements of the MIME body to the content type specified for the body.

If there is only one message body to be included in the third-party REGISTER request then the S-CSCF sets the Content-Type header field to the content type specified for the body.

#### 5.4.1.8 Service profile updates

NOTE 1: The S-CSCF can receive an update of subscriber data notification on the Cx interface, from the HSS, which can affect the stored information about served public user identities. According to 3GPP TS 29.228 [14], the changes are guaranteed not to affect the default public user identity within the registration implicit set.

When receiving a Push-Profile-Request (PPR) from the HSS (as described in 3GPP TS 29.228 [14]), modifying the service profile of served public user identities, the S-CSCF shall:

- 1) if the modification consists in the addition of a new non-barred public user identity to an implicit set, or in the change of status from barred to non-barred for a public user identity already in the implicit set, add the public user identity to the list of registered, non-barred public user identities;
- 2) if the modification consists in the deletion of a public user identity while there are no active multimedia session belonging to this public user identity, or in the change of status from non-barred to barred of a public user identity in an implicit set, remove the public user identity from the list of registered, non-barred public user identities;

NOTE 2: As the S-CSCF checks the barring status of the public user identity on receipt of a initial request for a dialog, or a standalone transaction, the above procedures have no impact on transactions or dialogs already in progress and are effective only for new transactions and dialogs.

- 3) if the modification consists of deletion of a public user identity from an implicit registration set while there are active multimedia session belonging to this public user identity and contact, release these multimedia sessions as described in subclause 5.4.5.1.2 and after all multimedia sessions are released, remove the public user identity from the list of registered, non-barred public user identities; and
- 4) synchronize with the UE and IM CN entities, by either:
  - performing the procedures for notification of the reg-event subscribers about registration state, as described in subclause 5.4.2.1.2; or
  - triggering the UE to re-register, by:
    - a) depending on operator configuration, rejecting a request from the UE using a 504 (Server Time-out) response and indicating in the response that S-CSCF restoration procedures are supported, in accordance with subclause 5.4.3.2; or
    - b) shortening the life time of the current registration, as described in subclause 5.4.1.6, e.g. when a new trigger point of Register method is added in the iFCs.

NOTE 3: The UE procedure in response to receiving a rejection as described in item a) (see subclause 5.1.2A.1.6) is specified for UEs since 3GPP Rel-8.

### 5.4.2 Subscription and notification

#### 5.4.2.1 Subscriptions to S-CSCF events

##### 5.4.2.1.1 Subscription to the event providing registration state

When an incoming SUBSCRIBE request addressed to S-CSCF arrives containing the Event header field with the reg event package, the S-CSCF shall:

- 1) check if, based on the local policy, the request was generated by a subscriber who is authorised to subscribe to the registration state of this particular user. The authorized subscribers include:
  - all public user identities this particular user owns, that the S-CSCF is aware of, and which are not-barred;
  - all the entities identified by the Path header field (i.e. the P-CSCF to which this user is attached to); and
  - all the ASs listed in the initial filter criteria that are part of the trust domain;

NOTE 1: The S-CSCF finds the identity for authentication of the subscription in the P-Asserted-Identity header field received in the SUBSCRIBE request.

- 1A) if the Request-URI of the SUBSCRIBE request identifies a public user identity that was implicitly registered using the registration procedures defined in RFC 6140 [191] and performs the functions of an external attached network, and the registration is currently active, then skip the remainder of the procedure in this subclause and route the SUBSCRIBE request to the UE performing the functions of an externally attached network using the procedures defined in subclause 5.4.3.3;
- 2) store the value of the "orig-ioi" header field parameter received in the P-Charging-Vector header field if present;

NOTE 2: Any received "orig-ioi" header field parameter will be a type 3 IOI. The type 3 IOI identifies the service provider from which the request was sent.

- 3) generate a 2xx response acknowledging the SUBSCRIBE request and indicating that the authorised subscription was successful as described in RFC 3680 [43]. The S-CSCF shall populate the header fields as follows:
  - an Expires header field, set to either the same or a decreased value as the Expires header field in SUBSCRIBE request; and
  - if the request originated from an ASs listed in the initial filter criteria, a P-Charging-Vector header field containing the "orig-ioi" header field parameter, if received in the SUBSCRIBE request, and a type 3 "term-ioi" header field parameter. The S-CSCF shall set the type 3 "term-ioi" header field parameter to a value that identifies the sending network of the response and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter.

The S-CSCF may set the Contact header field to an identifier uniquely associated to the SUBSCRIBE request and generated within the S-CSCF, that may help the S-CSCF to correlate refreshes for the SUBSCRIBE dialog; and

NOTE 3: The S-CSCF could use such unique identifiers to distinguish between UEs, when two or more users, holding a shared subscription, register under the same public user identity.

- 4) determine the applicable private user identity as the private user identity included in a REGISTER request:
  - which created (implicitly or explicitly) a binding of the public user identity in the Request-URI of the SUBSCRIBE request to an contact address; and
  - for which one of the following is true:
    - a) the 200 (OK) response to the REGISTER request contained the Service-Route header field with the S-CSCF URI matching the URI in the top Route header field of the SUBSCRIBE request (i.e. the SUBSCRIBE request originated by a served UE); or
    - b) the 200 (OK) response to the REGISTER request contained a Path header field with a URI matching the URI in the P-Asserted-Identity header field of the SUBSCRIBE request (i.e. the SUBSCRIBE request originated by a P-CSCF serving a UE).

NOTE 4: If the URI in the P-Asserted-Identity header field of the initial SUBSCRIBE request matches URIs of several Path header fields (e.g. the SUBSCRIBE request is originated by Rel-7 P-CSCF), the applicable private user identity is not determined.

Afterwards the S-CSCF shall perform the procedures for notification about registration state as described in subclause 5.4.2.1.2.

If the SUBSCRIBE request originated from an AS listed in the initial filter criteria, for any final response that is not a 2xx response, the S-CSCF shall insert a P-Charging-Vector header field containing the "orig-ioi" header field

parameter, if received in the SUBSCRIBE request and a type 3 "term-ioi" header field parameter. The S-CSCF shall set the type 3 "term-ioi" header field parameter to a value that identifies the sending network of the response and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter.

When the S-CSCF receives a subscription refresh request for a dialog that was established by the UE subscribing to the reg event package, the S-CSCF shall accept the request irrespective if the user's public user identity specified in the SUBSCRIBE request is either registered or has been deregistered.

#### 5.4.2.1.2 Notification about registration state

The UE can bind any one of its public user identities either to its contact address or to a registration flow and the associated contact address (if the multiple registration mechanism is used) via a single registration procedure. When multiple registrations mechanism is used to register a public user identity and bind it to a registration flow and the associated contact address, the S-CSCF shall generate a NOTIFY request that includes one <contact> element for each binding between a public user identity and a registration flow and the associated contact address.

NOTE 1: If the UE binds a given public user identity to the same contact address but several registration flows and the associated contact address (via several registrations), then the NOTIFY request will contain one <contact> element for each registration flow and the associated contact address. Each respective <contact> elements will contain the same contact address in the "uri" sub-element, but different value in the "id" sub-element and different "reg-id" value included in the respective <unknown-param> element.

For every successful registration that creates a new binding between a public user identity and either its contact address or the registration flow and the associated contact address (if the multiple registration mechanism is used, the NOTIFY request shall always include a new <contact> element containing new value in the "id" sub-element, the state attribute set to "active", and event attribute set to either "registered" or "created".

Any successful registration (that creates a new binding between a public user identity and either its contact address or a registration flow and associated contact address) may additionally replace or remove one or more existing bindings. In the NOTIFY request, for each replaced or removed binding, the <contact> element shall have the state attribute set to "terminated" and the event attribute set to "unregistered", "deactivated", or "rejected".

NOTE 2: When multiple registrations mechanism is not used, if the UE registers new contact address then all registrations, if any, using an old contact address are deregistered, i.e. the new registration replaces the old registrations. Hence, for each deregistered public user identity, the NOTIFY request will have the state attribute within the <registration> element set to "terminated" and the state attribute in the <contact> element set to "terminated" and the event attribute set to "unregistered", "deactivated", or "rejected".

NOTE 3: If the UE uses a multiple registrations mechanism to bind a public user identity to a new registration flow the registration flow and the associated contact address, and if the new registration flow replaces an existing registration flow, then for the registration flow and the associated contact address being replaced, the respective <contact> element in the NOTIFY request will have the state attribute set to "terminated" and the event attribute set to "unregistered", "deactivated", or "rejected".

The S-CSCF shall send a NOTIFY request:

- when an event pertaining to the user occurs. In this case the NOTIFY request is sent on all dialogs which have been established due to subscription to the reg event package of that user; and
- as specified in RFC 3265 [28].

When sending a NOTIFY request, the S-CSCF shall not use the default filtering policy as specified in RFC 3680 [43], i.e. the S-CSCF shall always include in every NOTIFY request the state information of all registered public user identities of the user (i.e. the full state information).

NOTE 4: Contact information related to emergency registration is not included.

When generating NOTIFY requests, the S-CSCF shall not preclude any valid reg event package parameters in accordance with RFC 3680 [43].

For each NOTIFY request triggered by an event and on all dialogs which have been established due to subscription to the reg event package of that user, the S-CSCF shall:

- 1) set the Request-URI and Route header field to the saved route information during subscription;

- 2) set the Event header field to the "reg" value;
- 3) in the body of the NOTIFY request, include one <registration> elements for each public user identity that the S-CSCF is aware the user owns.

If the user shares one or more public user identities with other users, the S-CSCF shall include any contact addresses registered by other users of the shared public user identity in the NOTIFY request;

- 4) for each <registration> element:
  - a) set the aor attribute to one public user identity or if the public user identity of this <registration> element is a wildcarded public user identity, then choose arbitrarily a public user identity that matches the wildcarded public user identity and the service profile of the wildcarded public user identity and set the aor attribute to this public user identity;

NOTE 5: The value of the aor attribute will not be used by the receiver of the NOTIFY.

- b) set the <uri> sub-element inside each <contact> sub-element of the <registration> element to the contact address provided by the respective UE as follows:
  - I) if the aor attribute of the <registration> element contains a SIP URI and if the Contact URI did not contain a "bnc" SIP URI parameter, then for each contact address that contains a "+sip.instance" Contact header field parameter, include <pub-gruu> and <temp-gruu> sub-elements within the corresponding <contact> element. The S-CSCF shall set the contents of these elements as specified in RFC 5628 [94]; or
  - II) if the aor attribute of the <registration> element contains a tel-URI, determine its alias SIP URI and if the Contact URI did not contain a "bnc" SIP URI parameter then include a copy of the <pub-gruu> and <temp-gruu> sub-elements from that equivalent element;
- c) if the respective UE has provided a display-name in a Contact header field, set the <display-name> sub-element inside the respective <contact> sub-element of the <registration> element to the value provided by the UE according to RFC3680 [43];
- d) if the user owns a wildcarded public user identity then include a <wildcardedIdentity> sub-element as described in subclause 7.10.2; and
- e) if the public user identity set in step a):
  - I) has been deregistered either by the UE or the S-CSCF (i.e. upon the deregistration, there are no binding left between this public user identity and either a contact address or a registration flows and associated contact addresses that belong to this user) then:
    - set the state attribute within the <registration> element to "terminated";
    - set the state attribute within each <contact> element belonging to this user to "terminated"; and
    - set the event attribute within each <contact> element to "deactivated", "expired", "unregistered", "rejected" or "probation" according to RFC 3680 [43].

If the public user identity has been deregistered for this user and this deregistration has already been indicated in the NOTIFY request, and no new registration for this user has occurred, its <registration> element shall not be included in the subsequent NOTIFY requests; or

- II) has been registered by the UE (i.e. the public user identity has not been previously bound either to a contact address or to a registration flow and the associated contact address (if the multiple registration mechanism is used)) then:
  - set the <unknown-param> element to any additional header field parameters contained in the Contact header field of the REGISTER request according to RFC 3680 [43];

NOTE 6: If the multiple registration mechanism is used, then the reg-id header field parameter will be included as an <unknown-param> element.

- if the subscription contains, for the applicable private user identity (determined as described in subclause 5.4.2.1.1) and the public user identity, any of the policies described in subclause 7.10.3,



then include the policy associated with the applicable private user identity and the public user identity using coding described in subclause 7.10.3;

- set the state attribute within the <registration> element to "active"; and:
- set the state attribute within the <contact> element belonging to this user to "active", include new value in the "id" sub-element, and set the event attribute within this <contact> element to "registered"; or

NOTE 7: If this registration, that created new binding, additionally replaces or removes one or more existing registrations, then for the replaced or removed registrations the respective <registration> elements and <contact> elements will be modified accordingly.

III) has been re-registered (i.e. it has been previously registered) then:

- set the state attribute within the <registration> element to "active";
- if the subscription contains, for the applicable private user identity (determined as described in subclause 5.4.2.1.1) and the public user identity, any of the policies described in subclause 7.10.3, then include the policy associated with the applicable private user identity and the public user identity using coding described in subclause 7.10.3;
- set the <unknown-param> element to any additional header field parameters contained in the Contact header field of the REGISTER request according to RFC 3680 [43];
- for contact addresses to be registered: set the state attribute within the <contact> element to "active"; and set the event attribute within the <contact> element to "registered"; or
- for contact addresses to be re-registered, set the state attribute within the <contact> element to "active"; and set the event attribute within the <contact> element to "refreshed" or "shortened" according to RFC 3680 [43]; or
- for contact addresses that remain unchanged, if any, leave the <contact> element unmodified (i.e. the event attribute within the <contact> element includes the last event that caused the transition to the respective state); or

IV) has been automatically registered or registered by the S-CSCF, and has not been previously automatically registered:

- set the <unknown-param> element to any additional header field parameters contained in the Contact header field of the REGISTER request according to RFC 3680 [43];
- set the state attribute within the <registration> element to "active";
- set the state attribute within the <contact> element to "active"; and
- set the event attribute within the <contact> element to "created"; and

V) is hosted (unregistered case) at the S-CSCF:

- set the state attribute within the <registration> element to "terminated";
- set the state attribute within each <contact> element to "terminated"; and
- set the event attribute within each <contact> element to "unregistered".

The S-CSCF shall also terminate the subscription to the registration event package by setting the Subscription-State header field to the value of "terminated"; and

NOTE 8: The value of "init" for the state attribute within the <registration> element is not used.

- f) set the callid and cseq attributes for the <contact> as specified in RFC 3680 [43], and the first-cseq attribute as specified in RFC 5628 [94].

NOTE 9: Errata of RFC 5628 clarifies the usage of the first-cseq attribute of the <temp-gruu> element.

- 5) set the P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17], and if the NOTIFY request is sent towards an AS listed in the initial filter criteria a type 3 "orig-ioi" header field parameter. The S-CSCF shall set the type 3 "orig-ioi" header field parameter to a value that identifies the sending network of the request. The S-CSCF shall not include the type 3 "term-ioi" header field parameter.

NOTE 10: When sending a NOTIFY request to a subscriber subscribing or unsubscribing to the reg event package, or when the S-CSCF terminates the subscription, the event attribute within the <contact> element includes the last event that caused the transition to the respective state.

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

EXAMPLE 1: If sip:user1\_public1@home1.net is registered, the public user identity sip:user1\_public2@home1.net can automatically be registered. Therefore the entries in the body of the NOTIFY request look like:

```
<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
  xmlns:cp="urn:ietf:params:xml:ns:common-policy"
  xmlns:eri="urn:3gpp:ns:extRegInfo:1.0"
  version="0" state="full">
  <registration aor="sip:user1_public1@home1.net" id="as9"
    state="active">
    <contact id="76" state="active" event="registered">
      <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
      <unknown-param name="audio"/>
    </contact>
  </registration>
  <registration aor="sip:user1_public2@home1.net" id="as10"
    state="active">
    <contact id="86" state="active" event="created">
      <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
      <unknown-param name="audio"/>
    </contact>
    <cp:actions>
      <eri:rph ns="wps" val="1"/>
      <eri:privSender/>
    </cp:actions>
  </registration>
</reginfo>
```

EXAMPLE 2: If sip:user1\_public1@home1.net is registered, the public user identity sip:ep\_user1@home1.net can automatically be registered. sip:ep\_user1@home1.net is a dedicated identity out of the related range indicated in the <wildcardedIdentity> element. Therefore the entries in the body of the NOTIFY request look like:

```
<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
  xmlns:ere="urn:3gpp:ns:extRegExp:1.0"
  version="0" state="full">
  <registration aor="sip:user1_public1@home1.net" id="as10"
    state="active">
    <contact id="86" state="active" event="created">
      <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
    </contact>
  </registration>
  <registration aor="sip:ep_user1@home1.net" id="as11"
    state="active">
    <contact id="86" state="active" event="created">
      <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
    </contact>
    <ere:wildcardedIdentity>sip:ep_user!.*!@home1.net
    </ere:wildcardedIdentity>
  </registration>
</reginfo>
```

When sending a final NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities have been deregistered, expired or are hosted (unregistered case) at the S-CSCF), the S-CSCF shall also terminate the subscription to the registration event package by setting the Subscription-State header field to the value of "terminated".

When all of a UE's contact addresses have been deregistered (i.e. there is no <contact> element set to "active" for this UE), the S-CSCF shall consider subscription to the reg event package belonging to the UE cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header field containing a value of zero).

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

When the S-CSCF receives any response to the NOTIFY request, the S-CSCF shall store the value of the "term-ioi" header field parameter received in the P-Charging-Vector header field, if present.

NOTE 11: Any received "term-ioi" header field parameter will be a type 3 IOI. The type 3 IOI identifies the service provider from which the response was sent.

5.4.2.1.3 Void

5.4.2.1.4 Void

### 5.4.2.1A Outgoing subscriptions to load-control event

Based on operator policy, the S-CSCF may subscribe to the load-control event package with one or more target SIP entities. The list of target SIP entities is provisioned.

Subscription to the load-control event package is triggered by internal events (e.g. the physical device hosting the SIP entity is power-cycled) or through a management interface.

The S-CSCF shall perform subscriptions to the load-control event package to a target entity in accordance with RFC 3265 [28] and with RFC 7200 [201]. When subscribing to the load-control event, the S-CSCF shall:

- 1) Send a SUBSCRIBE request in accordance with RFC 3265 [28] and with RFC 7200 [201] to the target entity, with the following elements:
  - an Expires header field set to a network specific value;
- 2) If the target entity is located in a different network and local policy requires the application of IBCF capabilities, forward the request to an IBCF acting as an exit point.

The S-CSCF shall automatically refresh ongoing subscription to the load-control event package either 600 seconds before the expiration time if the initial subscription was for greater than 1200 seconds, or when half of the time has expired if the initial subscription was for 1200 seconds or less.

The S-CSCF can terminate a subscription according to RFC 3265 [28].

### 5.4.2.2 Other subscriptions

Upon receipt of a NOTIFY request with the Subscription-State header field set to "terminated" and the S-CSCF has retained the SIP dialog state information for the associated subscription, once the NOTIFY transaction is terminated, the S-CSCF can remove all the stored information related to the associated subscription.

## 5.4.3 General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF

### 5.4.3.1 Determination of UE-originated or UE-terminated case

Upon receipt of an initial request or a stand-alone transaction, the S-CSCF shall:

- perform the procedures for the UE-originating case as described in subclause 5.4.3.2 if the request makes use of the information for UE-originating calls, which was added to the Service-Route header field entry of the S-CSCF during registration (see subclause 5.4.1.2), e.g. the message is received at a certain port or the topmost Route header field contains a specific user part or parameter; or,
- perform the procedures for the UE-originating case as described in subclause 5.4.3.2 if the topmost Route header field of the request contains the "orig" parameter. The S-CSCF shall remove the "orig" parameter from the topmost Route header field; or,
- perform the procedures for the UE-terminating case as described in subclause 5.4.3.3 if this information is not used by the request.

### 5.4.3.2 Requests initiated by the served user

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field or a temporarily authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the S-CSCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs.

NOTE 1: The special treatment can include filtering, higher priority processing, routing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

When the S-CSCF receives from the UE an initial request for a dialog, which contains a GRUU and an "ob" SIP URI parameter in the Contact header field, and multiple contact addresses have been registered for the specific GRUU, then for all subsequent in-dialog requests sent toward the UE's, the S-CSCF shall populate the Request-URI with the registered contact address from which the UE sent the initial request for the dialog.

NOTE 2: When a given contact address is registered, the S-CSCF can use a dedicated value in its Service-Route header field entry to identify the given contact address. When the S-CSCF receives an initial request for a dialog, the S-CSCF can find out from which contact address the initial request was sent by looking at the preloaded Route header field (constructed from the Service-Route header field returned in the response for the REGISTER request) which contains the entry of the S-CSCF.

When performing SIP digest without TLS, when the S-CSCF receives from the served user an initial request for a dialog or a request for a standalone transaction, the S-CSCF may perform the steps in subclause 5.4.3.6 to challenge the request based on local policy.

NOTE 3: If the user registration is associated with the state "tls-protected", then the execution of Proxy-Authorization as described in subclause 5.4.3.6 is still possible, although it is unlikely this would add additional security provided the P-CSCF is trusted. Thus, in most cases the state "tls-protected" will be reason for the S-CSCF to not desire Proxy-Authentication for this user.

NOTE 4: The option for the S-CSCF to challenge the request does not apply to a request from an AS acting as an originating UA.

When performing GPRS-IMS-Bundled authentication, when the S-CSCF receives from the served user an initial request for a dialog or a request for a standalone transaction, the S-CSCF shall check whether a "received" header field parameter exists in the Via header field provided by the UE. If a "received" header field parameter exists, S-CSCF shall compare the (prefix of the) IP address received in the "received" header field parameter against the UE's IP address (or prefix) stored during registration. If no "received" header field parameter exists in the Via header field provided by the UE, then S-CSCF shall compare the (prefix of the) IP address received in the "sent-by" parameter against the IP address (or prefix) stored during registration. If the stored IP address (or prefix) and the (prefix of the) IP address in the "received" Via header field parameter provided by the UE do not match, the S-CSCF shall reject the request with a 403 (Forbidden) response. In case the stored IP address (or prefix) and the (prefix of the) IP address in the "received" Via header field parameter provided by the UE do match, the S-CSCF shall proceed as described in the remainder of this subclause.

When the S-CSCF receives from the served user or from a PSI an initial request for a dialog or a request for a standalone transaction, and the request is received either from a functional entity within the same trust domain or contains a valid original dialog identifier (see step 3) or the dialog identifier (From, To and Call-ID header fields) relates to an existing request processed by the S-CSCF, then prior to forwarding the request, the S-CSCF shall:

- 0) if the request is received from a P-CSCF that does not support the trust domain handling of the P-Served-User header field then remove any P-Served-User header fields;
- 1) determine the served user as follows:
  - a) if the request contains a P-Served-User header field then
    - i) determine the served user by taking the identity contained in a P-Served-User header field as defined in RFC 5502 [133]. Then check whether the determined served user is a barred public user identity. In case the said header field contains the served user identity is a barred public user identity for the user, then the

S-CSCF shall reject the request by generating a 403 (Forbidden) response. Otherwise, the S-CSCF shall save the public user identity of the served user and continue with the rest of the steps;

- b) if the request does not contain a P-Served-User header field then
- i) determine the served user by taking the identity contained in one of the URI(s) of the P-Asserted-Identity header field. In case the determined served user is a barred public user identity, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. Otherwise, the S-CSCF shall save the public user identity of the served user and continue with the rest of the steps; and
  - ii) if the P-Asserted-Identity header field contains two URIs and the URI other than the determined served user is not an alias of the determined served user or is barred then act based on local policy, e.g. reject the request by generating a 403 (Forbidden) response or remove the URI not identifying the determined served user from the P-Asserted-Identity header field;

NOTE 5: If the P-Asserted-Identity header field contains a barred public user identity, then the message has been received, either directly or indirectly, from a non-compliant entity which should have had generated the content with a non-barred public user identity.

- 1A) if the Contact is a GRUU, but is not valid as defined in subclause 5.4.7A.4, then return a 4xx response as specified in RFC 5627 [93];
- 2) store the value of the "orig-oi" header field parameter received in the P-Charging-Vector header field if present, and remove it from any forwarded request;

NOTE 6: Any received "orig-oi" header field parameter will be a type 3 IOI. The type 3 IOI identifies the service provider from which the request was sent (AS initiating a session on behalf of a user or a PSI);

- 3) check if an original dialog identifier that the S-CSCF previously placed in a Route header field is present in the topmost Route header field of the incoming request.
- If not present, the S-CSCF shall build an ordered list of initial filter criteria based on the public user identity of the served user (as determined in step 1) of the received request as described in 3GPP TS 23.218 [5].
  - If present, the request has been sent from an AS in response to a previously sent request, an ordered list of initial filter criteria already exists and the S-CSCF shall not change the ordered list of initial filter criteria even if the AS has changed the P-Served-User header field or the P-Asserted-Identity header field;

NOTE 7: An original dialog identifier is sent to each AS invoked due to iFC evaluation such that the S-CSCF can associate requests as part of the same sequence that trigger iFC evaluation in priority order (and not rely on SIP dialog information that can change due to B2BUA AS). If the same original dialog identifier is included in more than one request from a particular AS (based on service logic in the AS), then the S-CSCF will continue the iFC evaluation sequence rather than build a new ordered list of iFC;

- 4) remove its own SIP URI from the topmost Route header field;

4A) if a reference location was received from the HSS at registration as part of the user profile and the request does not contain a message body with the content type application/pdf+xml in accordance with RFC 6442 [89], the S-CSCF shall insert a P-Access-Network-Info header field constructed according to the reference location received from the HSS and containing the "network-provided" parameter. The P-Access-Network-Info header shall only be inserted if there is not already a network provided information. The access type information received from the HSS shall be mapped into the corresponding access-type parameter of the P-Access-Network-Info header field and the location information shall be mapped into the location parameter corresponding to the access-type parameter, i.e. into "dsl-location" parameter, "fiber-location" parameter or "eth-location" parameter;

4B) if there was an original dialog identifier present in the topmost Route header field of the incoming request and the request is received from a functional entity within the same trust domain and contains a P-Asserted-Service header field, continue the procedure with step 5;

4C) if the request contains a P-Preferred-Service header field, check whether the ICSI value contained in the P-Preferred-Service header field is part of the set of the subscribed services for the served user and determine whether the contents of the request (e.g. SDP media capabilities, Content-Type header field) match the ICSI for the subscribed service:

- a) if not, as an operator option, the S-CSCF may reject the request by generating a 403 (Forbidden) response. Otherwise remove the P-Preferred-Service header field and continue with the rest of the steps; and
  - b) if so, then include a P-Asserted-Service header field in the request containing the ICSI value contained in the P-Preferred-Service header field, remove the P-Preferred-Service header field, and continue the procedure with step 5;
- 4D) if the request does not contain a P-Preferred-Service header field, check whether the contents of the request match a subscribed service for each and any of the subscribed services for the served user:
- a) if not, as an operator option, the S-CSCF may reject the request by generating a 403 (Forbidden) response; and
  - b) if so, and if the request is related to an IMS communication service and the IMS communication service requires the use of an ICSI value then select an ICSI value for the related IMS communication service and include a P-Asserted-Service header field in the request containing the selected ICSI value; and

NOTE 8: If more than one ICSI values match the contents of the request, the S-CSCF selects an ICSI value based on local policy.

- c) if so, and if the request is related to an IMS communication service and the IMS communication service does not require the use of an ICSI value then continue without including an ICSI value; and
  - d) if so, and if the request does not relate to an IMS communication service (or if the S-CSCF is unable to unambiguously determine the service being requested but decides to allow the session to continue) then continue without including an ICSI value;
- 5) check whether the initial request matches any unexecuted initial filter criteria. If there is a match, then the S-CSCF shall select the first matching unexecuted initial filter criteria from the ordered list of initial filter criteria and the S-CSCF shall:
- a) insert the AS URI to be contacted into the Route header field as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

NOTE 9: If the AS is accessed via an ISC gateway function, then the URI will be the address of the ISC gateway function.

- b) if the S-CSCF supports the P-Served-User extension as specified in RFC 5502 [133] and draft-ietf-sipcore-originating-cdiv-parameter [239] insert P-Served-User header field populated with the served user identity as determined in step 1. If required by operator policy, the S-CSCF shall:
  - if the associated session case is "Originating" as specified in 3GPP TS 29.228 [14], include the sescase header field parameter set to "orig" and the regstate header field parameter set to "reg";
  - if the associated session case is "Originating\_Unregistered" as specified in 3GPP TS 29.228 [14], include the sescase header field parameter set to "orig" and the regstate header field parameter set to "unreg";
  - if the associated session case is "Originating\_CDIV" as specified in 3GPP TS 29.228 [14], include the "orig-cdiv" header field parameter, defined in draft-ietf-sipcore-originating-cdiv-parameter [239]; and
- c) if the AS is located outside the trust domain then the S-CSCF shall remove the access-network-charging-info parameter in the P-Charging-Vector header field from the request that is forwarded to the AS; if the AS is located within the trust domain, then the S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header field in the request that is forwarded to the AS; and
- d) insert a type 3 "orig-ioi" header field parameter in place of any received "orig-ioi" header field parameters in the P-Charging-Vector header field. The S-CSCF shall set the type 3 "orig-ioi" header field parameter to a value that identifies the sending network of the request. The S-CSCF shall not include the type 3 "term-ioi" header field parameter;

NOTE 10: Depending on the result of processing the filter criteria the S-CSCF might contact one or more AS(s) before processing the outgoing Request-URI.

NOTE 11: An AS can activate or deactivate its own filter criteria via the Sh interface. As the S-CSCF checks initial filter criteria only on receipt of an initial request for a dialog, or a standalone transaction, a modified service profile will have no impact on transactions or dialogs already in progress and the modified profile will be effective only for new transactions and dialogs. If the S-CSCF receives a modification of the iFC during their execution, then it should not update the stored initial Filter Criteria until the iFC related to the initial request have been completely executed.

- 6) if there was no original dialog identifier present in the topmost Route header field of the incoming request store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field and retain the "icid-value" header field parameter in the P-Charging-Vector header field. Optionally, the S-CSCF may generate a new, globally unique ICID and insert the new value in the "icid-value" header field parameter of the P-Charging-Vector header field when forwarding the message. If the S-CSCF creates a new ICID, then it is responsible for maintaining the two ICID values in the subsequent messaging;
- 7) in step 5, if the initial request did not match any unexecuted initial filter criteria (i.e. the request is not forwarded to an AS), insert a type 2 "orig-ioi" header field parameter into the P-Charging-Vector header field. The S-CSCF shall set the type 2 "orig-ioi" header field parameter to a value that identifies the sending network. The S-CSCF shall not include the type 2 "term-ioi" header field parameter;
- 8) insert a P-Charging-Function-Addresses header field populated with values received from the HSS if the request does not contain a P-Charging-Function-Addresses header field and the message is forwarded within the S-CSCF home network, including towards AS;
- 9) if there was no original dialog identifier present in the topmost Route header field of the incoming request and if the served user is not considered a privileged sender then:
  - a) if the P-Asserted-Identity header field contains only a SIP URI and if the S-CSCF has knowledge that the SIP URI contained in the received P-Asserted-Identity header field is an alias SIP URI for a tel URI, add a second P-Asserted-Identity header field containing this tel-URI, including the display name associated with the tel URI, if available; and
  - b) if the P-Asserted-Identity header field contains only a tel URI, the S-CSCF shall add a second P-Asserted-Identity header field containing a SIP URI. The added SIP URI shall contain in the user part a "+" followed by the international public telecommunication number contained in tel URI, and user's home domain name in the hostport part. The added SIP URI shall contain the same value in the display name as contained in the tel URI. The S-CSCF shall also add a "user" SIP URI parameter equals "phone" to the SIP URI;

NOTE 12: If tel URI is shared URI so is the alias SIP URI.

10) if the request is not forwarded to an AS and if the outgoing Request-URI is:

- a SIP URI with the user part starting with a + and the "user" SIP URI parameter equals "phone", and if configured per local operator policy, the S-CSCF shall perform the procedure described here. Local policy can dictate whether this procedure is performed for all domains of the SIP URI, only if the domain belongs to the home network, or not at all. If local policy indicates that the procedure is to be performed, then the S-CSCF shall translate the international public telecommunications number contained in the user part of the SIP URI (see RFC 3966 [22]) to a globally routeable SIP URI using either an ENUM/DNS translation mechanism with the format specified in RFC 6116 [24], or any other available database. Database aspects of ENUM are outside the scope of the present document. An S-CSCF that implements the additional routing functionality described in annex I may forward the request without attempting translation. If an agreement exists between the home network and the visited network to support roaming architecture for voice over IMS with local breakout, the S-CSCF does not enable NP capabilities, and the S-CSCF decides to loopback the call to the visited network, the S-CSCF may forward the request without attempting translation. If a translation is in fact performed and it succeeds, the S-CSCF shall update the Request-URI with the globally routeable SIP URI either returned by ENUM/DNS or obtained from any other available database. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g. a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator. When forwarding the request to a BGCF or any other appropriate entity, the S-CSCF shall leave the original Request-URI containing the SIP URI with "user" SIP URI parameter equals phone unmodified. If the request is forwarded, the S-CSCF shall remove the access-network-charging-info parameter from the P-Charging-Vector header field prior to forwarding the message;
- a SIP URI with a "user" SIP URI parameter equals "dialstring" and the domain name of the SIP URI belongs to the home network (i.e. the local number analysis and handling is either failed in the appropriate AS or the

request has not been forwarded to AS for local number analysis and handling at all), either forward the request to any appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or send an appropriate SIP response to the originator;

- a SIP URI with a local number (see RFC 3966 [22]) in the user part and a "user" SIP URI parameter equals "phone" and the domain name of the SIP URI belongs to the home network (i.e. the local number analysis and handling is either failed in the appropriate AS or the request has not been forwarded to AS for local number analysis and handling at all), either forward the request to a BGCF for any appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or send an appropriate SIP response to the originator;
- a tel URI containing a global number (see RFC 3966 [22]) in the international format, the S-CSCF shall translate the E.164 address to a globally routeable SIP URI using either an ENUM/DNS translation mechanism with the format specified in RFC 6116 [24], or any other available database. Database aspects of ENUM are outside the scope of the present document. An S-CSCF that implements the additional routing functionality described in Annex I may forward the request without attempting translation. If an agreement exists between the home network and the visited network to support roaming architecture for voice over IMS with local breakout, the S-CSCF does not enable NP capabilities, and the S-CSCF decides to loopback the call to the visited network, the S-CSCF may forward the request without attempting translation. If this translation is in fact performed and it succeeds, the S-CSCF shall update the Request-URI with the globally routeable SIP URI returned by ENUM/DNS or any other available database. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator. When forwarding the request to a BGCF or any other appropriate entity, the S-CSCF shall leave the original Request-URI containing the tel URI unmodified. If the request is forwarded, the S-CSCF shall remove the access-network-charging-info parameter from the P-Charging-Vector header field prior to forwarding the message;
- a tel URI containing a local number (see RFC 3966 [22]) (i.e. the local number analysis and handling is either failed in the appropriate AS or the request has not been forwarded to AS for local number analysis and handling at all), either forward the request to a BGCF or any other appropriate entity (e.g. a MRFC to play an announcement) in the originator's home network or send an appropriate SIP response to the originator;
- a pres URI or an im URI, the S-CSCF shall forward the request as specified in RFC 3861 [63]. In this case, the S-CSCF shall not modify the received Request-URI: and
- a service URN, e.g. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]. In this case the S-CSCF shall not modify the received Request-URI.

NOTE 13: If there is no SIP-based transport found after applying the procedure specified in RFC 3861 [63], the S-CSCF can forward the request to a translating gateway.

Additional procedures apply if the S-CSCF supports NP capabilities and these capabilities are enabled by local policy, and the database used for translation from an international public telecommunications number to a SIP URI also provides NP data (for example, based on the PSTN Enumservice as defined by RFC 4769 [114] or other appropriate data bases). If the above translation from an international public telecommunications number to a SIP URI failed, but NP data was obtained from the database and there is no "npdi" parameter in the received request, then the S-CSCF shall, based on operator policy, update the URI in the Request-URI with the obtained NP data, prior to forwarding the request to the BGCF or other appropriate entity. If the received request already contains a tel-URI "npdi" parameter, then the S-CSCF may update the URI with the obtained NP data. The URI is updated by the S-CSCF by adding NP parameters defined by RFC 4694 [112]. If the Request-URI is a tel-URI, then an "npdi" tel-URI parameter is added to indicate that NP data retrieval has been performed, and if the number is ported, an "rn" tel-URI parameter is added to identify the ported-to routing number. If the Request-URI is in the form of a SIP URI user=phone, the "npdi" and "rn" tel-URI parameters are added as described above to the userinfo part of the SIP URI;

- 10A) if the request is not forwarded to an AS and if local policy requires the application of additional routing capabilities, as defined in Annex I, the S-CSCF shall apply the additional routing capabilities if they are locally available or forward the request to an entity that implements the additional routing capabilities;
- 10B) if an agreement exists between the home network and the visited network to support Roaming Architecture for Voice over IMS with Local Breakout then continue with the following steps. Otherwise continue with step 11. If:



- the top most Route header contains an indication that this is the UE-originating case;

NOTE 14: This indication can e.g. be in a URI parameter, a character string in the user part of the URI or can be a port number in the URI added by the S-CSCF during the registration in the Service-Route header field.

- the UE is roaming (as identified by the P-Visited-Network-ID header field value in the original REGISTER request); and
- the request is an INVITE request;

determine if loopback routing is applicable for this request using local policy, and save this decision for subsequent processing along with the following information:

- a) any URI representing the TRF address preference received from the visited network; and
- b) the ICID received in the request.

In addition, the S-CSCF shall also include in the request a Feature-Caps header field with the "+g.3gpp.home-visited" header field parameter according to RFC 6809 [190] with the "+g.3gpp.home-visited" header field parameter set to the identifier of the visited network received in the P-Visited-Network-ID header field in the original registration request;

10C) if the request is an INVITE request, then determine whether loopback is applied for this request. The information saved in step 10B, and the presence or absence of the Feature-Caps header field with the "+g.3gpp.home-visited" header field parameter in the received INVITE request are taken into account in making this decision:

- a) if loopback routing is not to be performed for this request remove any "+g.3gpp.trf" header field parameter or "+g.3gpp.home-visited" header field parameter from the Feature-Caps header field of the outgoing request;
- b) if loopback routing is applied for this request;
  - i) remove all entries in the Route header field;
  - ii) if a "+g.3gpp.trf" header field parameter with a parameter value containing a valid URI, is included in the Feature-Caps header field of the request, insert the URI in a Route header field;
  - iii) if a "+g.3gpp.trf" header field parameter, with a parameter value containing a valid URI is not included in the Feature-Caps header field of the request, insert a locally configured TRF address, associated with the visited network for this call, in the Route header field;
  - iv) remove any "+g.3gpp.home-visited" header field parameter from the Feature-Caps header field of the outgoing request;
  - v) insert the "+g.3gpp.loopback" header field parameter as described in subclause 7.9A.4 in the Feature-Caps header field of the request, in accordance with RFC 6809 [190]. If providing the identifier of the home network is supported by the S-CSCF and the visited network, the S-CSCF may based on operator agreement insert the "+g.3gpp.loopback" header field parameter set to the identifier of the home network;
  - vi) if included in the incoming request, remove the "+g.3gpp.trf" header field parameter from the Feature-Caps header field from the outgoing request; and
  - vii) remove a type 2 "orig-ioi" header field parameter that was added in step 7 from the P-Charging-Vector header field and insert a type 1 "orig-ioi" header field parameter into the P-Charging-Vector header field. The S-CSCF shall set the type 1 "orig-ioi" header field parameter to a value that identifies the network in which the S-CSCF resides. The S-CSCF shall not include the "term-ioi" header field parameter; and
- c) if the final decision on loopback routing is deferred to a subsequent entity in the home network, the BGCF, then the S-CSCF includes, if absent, in the request a Feature-Caps header field with the "+g.3gpp.home-visited" header field parameter, with the parameter value set to the identifier of the visited network received in the P-Visited-Network-ID header field in the original registration request. The S-CSCF is expected to know by means of network configuration that such a subsequent entity exists; and

NOTE 15: The subsequent entity in the home network, the BGCF, will remove the "+g.3gpp.home-visited" header field parameter from the Feature-Caps header field when a final routing decision is taken.

11) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header field if present, otherwise based on the Request-URI. If the destination requires interconnect functionalities (e.g. the destination address is of an IP address type other than the IP address type used in the IM CN subsystem), the S-CSCF shall forward the request to the destination address via an IBCF in the same network;

12) if network hiding is needed due to local policy, put the address of the IBCF to the topmost Route header field;

13) in case of an initial request for a dialog:

a) determine the need for GRUU processing. GRUU processing is required if:

- an original dialog identifier that the S-CSCF previously placed in a Route header field is not present in the topmost Route header field of the incoming request (this means the request is not returning after having been sent to an AS), and
- the contact address contains a GRUU that was either assigned by the S-CSCF that is valid as specified in subclause 5.4.7A.4 or a temporary GRUU self assigned by the UE based on the "temp-gruu-cookie" header parameter provided to the UE;

NOTE 16: The procedures for determining that a URI is a temporary GRUU assigned by the UE are specified in subclause 7.1.2.3 of RFC 6140 [191].

b) if GRUU processing is not required and the initial request originated from a served user, then determine the need to record-route for other reasons:

- if the request is routed to an AS which is part of the trust domain, the S-CSCF shall decide, based on operator policy, whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header field containing its own SIP URI;
- if the request is a SUBSCRIBE request and routed elsewhere, the S-CSCF shall decide, based on operator policy, whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request (e.g. event package name). If the request is record-routed the S-CSCF shall create a Record-Route header field containing its own SIP URI; or

NOTE 17: Some subscriptions to event packages (e.g. presence) can result in virtually persistent subscriptions and if the S-CSCF Record-Routes this can prevent reassignment of the S-CSCF.

NOTE 18: If the S-CSCF does not Record-Route the initial SUBSCRIBE request, it will not be possible to perform SIP digest authentication of SIP requests sent inside the SIP dialog related to the associated subscription.

- if the request not a SUBSCRIBE request and is routed elsewhere, create a Record-Route header field containing its own SIP URI;

NOTE 19: For requests originated from a PSI the S-CSCF can decide whether to record-route or not based on operator policy.

c) if GRUU processing is required, the S-CSCF shall create a Record-Route header field containing its own SIP URI;

d) if GRUU processing is required, the S-CSCF shall save an indication that GRUU-routing is to be performed for in-dialog requests that reach the S-CSCF because of the Record-route header field added in step c);

NOTE 20: The manner of representing the GRUU-routing indication is a private matter for the S-CSCF. The indication is used during termination processing of in-dialog requests to cause the S-CSCF to replace a Request-URI containing a GRUU with the corresponding registered contact address. It can be saved using values in the Record-Route header field, or in dialog state.

14) based on the destination user (Request-URI), remove any P-Access-Network-Info header field and the access-network-charging-info parameter in the P-Charging-Vector header field prior to forwarding the message;

14A) if the request is not routed to an AS, to a BGCF or to an entity that implements the additional routing functionality, remove the P-Served-User header field prior to forwarding the request;

15) route the request based on SIP routing procedures; and

- 16) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed.

When the S-CSCF receives, an initial request for a dialog or a request for a standalone transaction, from an AS acting on behalf of an unregistered user, the S-CSCF shall:

- 1) execute the procedures described in the steps 1, 2, 3, 4, 4B, 4C, 4D, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 and 16 in the above paragraph (when the S-CSCF receives, from a registered served user, an initial request for a dialog or a request for a standalone transaction).

NOTE 21: When the S-CSCF does not have the user profile, before executing the actions as listed above, it initiates the S-CSCF Registration/deregistration notification procedure, as described in 3GPP TS 29.228 [14]; with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informs the HSS that the user is unregistered. The S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14]. When requesting the user profile, and the request received by the S-CSCF contains a P-Profile-Key header field, the S-CSCF can include the header field value in S-CSCF Registration/deregistration notification. If the response from the HSS includes a Wildcarded Public Identity AVP, and if the request received by the S-CSCF did not include a P-Profile-Key header field, the S-CSCF uses the AVP value to set the P-Profile-Key header field before forwarding the request to an AS.

When the S-CSCF receives a request initiated by the served user for which the S-CSCF does not have the user profile or does not trust the data that it has (e.g. due to restart), the S-CSCF shall attempt to retrieve the user profile from the HSS. If the S-CSCF receives a Diameter result code of DIAMETER\_UNABLE\_TO\_COMPLY as defined in 3GPP TS 29.228 [14], the S-CSCF supports S-CSCF restoration procedures, and the Request-URI of the request does not match an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69], then the S-CSCF shall:

- I) reject the request by returning a 504 (Server Time-out) response to the UE;
- II) assume that the UE supports version 1 of the XML Schema for the 3GPP IM CN subsystem XML body if support for the 3GPP IM CN subsystem XML body as described in subclause 7.6 in the Accept header field is not indicated; and
- III) include in the 504 (Server Time-out) response:
  - a Content-Type header field with the value set to associated MIME type of the 3GPP IM CN subsystem XML body as described in subclause 7.6.1;
  - a P-Asserted-Identity header field set to the value of the SIP URI of the S-CSCF included in the Service-Route header field (see subclause 5.4.1.2.2F) during the registration of the user whose UE sent the request causing this response; and
  - a 3GPP IM CN subsystem XML body:
    - a) an <ims-3gpp> element with the "version" attribute set to "1" and with an <alternative-service> child element, set to the parameters of the alternative service;
      - i) a <type> child element, set to "restoration" (see table 7.6.2) to indicate that S-CSCF restoration procedures are supported;
      - ii) a <reason> child element, set to an operator configurable reason; and
      - iii) an <action> child element, set to "initial-registration" (see table 7.6.3).

NOTE 22: These procedures do not prevent the usage of unspecified reliability or recovery techniques above and beyond those specified in this subclause.

Depending on operator configuration (see subclause 5.4.1.8), when the S-CSCF receives a request with a Request-URI that does not match an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69], the request initiated by the served user for which the S-CSCF has modified but not synchronized the service profile for the served user and the S-CSCF supports S-CSCF restoration procedures, then the S-CSCF shall reject the request as described in items I), II) and III).

If the S-CSCF:

- a) fails to receive a SIP response within a configurable time; or

- b) receives a 408 (Request Timeout) response or a 5xx response from the AS without previously receiving a 1xx response to the original SIP request, and without previously receiving a SIP request from the AS that contained the same original dialog identifier as the original request;

the S-CSCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION\_CONTINUED" as specified in 3GPP TS 29.228 [14] or no default handling is indicated, execute the procedure from step 5; and
- if the default handling defined in the filter criteria indicates the value "SESSION\_TERMINATED" as specified in 3GPP TS 29.228 [14], either forward the received response or, if the request is an initial INVITE request, send a 408 (Request Timeout) response or a 5xx response towards the served UE as appropriate (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

If the S-CSCF receives any final response from the AS, the S-CSCF shall forward the response towards the served UE (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

When the S-CSCF receives any response to the above request, the S-CSCF may:

- 1) apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header field.

NOTE 23: The P-Asserted-Identity header field would normally only be expected in 1xx or 2xx responses.

NOTE 24: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

When the S-CSCF receives any response to the above request containing a "term-ioi" header field parameter, the S-CSCF shall store the value of the received "term-ioi" header field parameter received in the P-Charging-Vector header field, if present, and remove all received "orig-ioi", "term-ioi" and "transit-ioi" header field parameters from the forwarded response if next hop is not an AS.

NOTE 25: Any received "term-ioi" header field parameter will be a type 2 IOI, if received from an S-CSCF, or type 3 IOI, if received from an AS, or type 1 IOI if the S-CSCF performed loopback routing for this request. A type 2 IOI identifies the sending network of the response, a type 3 IOI identifies the sending service provider of the response, and a type 1 IOI identifies the visited network of the served user.

When the S-CSCF receives any response to the above request, and forwards it to AS, the S-CSCF shall remove all received "orig-ioi" and "term-ioi" header field parameters received in the P-Charging-Vector header field if present, and shall insert in the P-Charging-Vector header field the "orig-ioi" header field parameter, if received in the request, and a type 3 "term-ioi" header field parameter in the response. The S-CSCF shall set the type 3 "term-ioi" header field parameter to a value that identifies the sending network of the response and the type 3 "orig-ioi" header field parameter is set to the previously received value of type 3 "orig-ioi" header field parameter.

When the S-CSCF receives any 1xx or 2xx response to the initial request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response in order to be able to release the session if needed.

When the S-CSCF receives any 1xx or 2xx response to an initial request for a dialog or a request for a standalone transaction, if the response is forwarded within the S-CSCF home network and not to an AS, the S-CSCF shall insert a P-Charging-Function-Addresses header field populated with values received from the HSS.

When the S-CSCF, upon sending an initial INVITE request that includes an IP address in the SDP offer (in "c=" parameter), receives an error response indicating that the IP address type is not supported, (e.g., the S-CSCF receives the 488 (Not Acceptable Here) with 301 Warning header field indicating "incompatible network address format"), the S-CSCF shall either:

- fork the initial INVITE request to the IBCF; or
- process the error response and forward it using the Via header field.

NOTE 26: If the S-CSCF knows that the originating UE supports both IPv6 and IPv4 addresses simultaneously, the S-CSCF will forward the error response to the UE using the Via header field. The present version of the specification does not specify how the S-CSCF determines whether the UE supports both IPv6 and IPv4 addressing simultaneously.

When the S-CSCF receives from the served user a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

- 0A) if the dialog is related to an IMS communication service determine whether the contents of the request (e.g. SDP media capabilities, Content-Type header field) match the IMS communication service as received as the ICSI value in the P-Asserted-Service header field in the initial request. As an operator option, if the contents of the request do not match the IMS communication service the S-CSCF may reject the request by generating a status code reflecting which added contents are not matching. Otherwise, continue with the rest of the steps;
- 1) remove its own URI from the topmost Route header field;
- 2) create a Record-Route header field containing its own SIP URI;
- 3) for INVITE dialogs (i.e. dialogs initiated by an INVITE request), save the Contact and CSeq header field values received in the request such that the S-CSCF is able to release the session if needed;
- 4) in case the request is routed towards the destination user (Request-URI) or in case the request is routed to an AS located outside the trust domain, remove the access-network-charging-info parameter in the P-Charging-Vector header field; and
- 5) route the request based on the topmost Route header field.

When the S-CSCF receives any 1xx or 2xx response to the target refresh request for an INVITE dialog, the S-CSCF shall replace the saved Contact header field values in the response such that the S-CSCF is able to release the session if needed.

If the S-CSCF inserted in the initial request for the dialog the header field parameters into the Feature-Caps header field then the S-CSCF shall include the header field parameters with the same parameter values into the Feature-Caps header field in any target refresh request for the dialog, and in each 1xx or 2xx response to target refresh request sent in the same direction.

When the S-CSCF receives from the served user a subsequent request other than a target refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

- 1) remove its own URI from the topmost Route header field;
- 2) in case the request is routed towards the destination user (Request-URI) or in case the request is routed to an AS located outside the trust domain, remove the access-network-charging-info parameter in the P-Charging-Vector header field; and
- 3) route the request based on the topmost Route header field.

With the exception of 305 (Use Proxy) responses, the S-CSCF shall not recurse on 3xx responses.

### 5.4.3.3 Requests terminated at the served user

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field or a temporarily authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the S-CSCF shall give priority over other transactions or dialogs. This allows special treatment for such transactions or dialogs.

NOTE 1: The special treatment can include filtering, higher priority processing, routeing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

When the S-CSCF receives, destined for a registered served user, an initial request for a dialog or a request for a standalone transaction, and the request is received either from a functional entity within the same trust domain or contains a valid original dialog identifier or the dialog identifier (From, To and Call-ID header fields) relates to an existing request processed by the S-CSCF, then prior to forwarding the request, the S-CSCF shall:

- 1) check if an original dialog identifier that the S-CSCF previously placed in a Route header field is present in the topmost Route header field of the incoming request.

- If present, the request has been sent from an AS in response to a previously sent request.
- If not present, it indicates that the request is visiting the S-CSCF for the first time and in this case the S-CSCF shall determine the served user by taking the identity contained in the Request-URI. If the Request-URI is a temporary GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.3, then take the public user identity that is associated with the temporary GRUU to be the served user identity. Then check whether the determined served user identity is a barred public user identity. In case the served user identity is a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 404 (Not Found) response. Otherwise, the S-CSCF shall save the Request-URI from the request, the served user identity and the public user identity of the served user and continue with the rest of the steps;

NOTE 2: An original dialog identifier is sent to each AS invoked due to iFC evaluation such that the S-CSCF can associate requests as part of the same sequence that trigger iFC evaluation in priority order (and not rely on SIP dialog information that can change due to B2BUA AS). If the same original dialog identifier is included in more than one request from a particular AS (based on service logic in the AS), then the S-CSCF will continue the iFC evaluation sequence rather than build a new ordered list of iFC;

2) remove its own URI from the topmost Route header field;

2A) if there was no original dialog identifier present in the topmost Route header field of the incoming request build an ordered list of initial filter criteria based on the public user identity in the Request-URI of the received request as described in 3GPP TS 23.218 [5].

3) if there was an original dialog identifier present in the topmost Route header field of the incoming request then check whether the Request-URI matches the saved Request-URI. The Request-URI and saved Request-URI are considered a match:

- a) if the canonical forms of the two Request-URI are equal to the saved value of the Request-URI;
- b) if the Request-URI is a GRUU (public or temporary) and the saved value of the Request-URI is a GRUU (public or temporary) and both GRUUs represent the same public user identity; or
- c) if the Request-URI is an alias SIP URI of the saved value of the Request-URI.

NOTE 3: The canonical form of the Request-URI is obtained by removing all URI parameters (including the user-param), and by converting any escaped characters into unescaped form. The alias SIP URI is defined in subclause 3.1.

If there is no match, then the S-CSCF shall decide whether to trigger the originating services to be executed after retargeting. The decision is configured in the S-CSCF and may use any information in the received request that is used for the initial filter criteria or an operator policy. The S-CSCF shall decide either to:

- a) stop evaluating current iFC. In that case, if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed, forward the request based on the topmost Route header field or if not available forward the request based on the Request-URI (routing based on Request-URI is specified in steps 7 and 10 through 14a from subclause 5.4.3.2) and skip the following steps; or
- b) stop evaluating current iFC and build an ordered list of iFC with the originating services to be executed after retargeting as described in 3GPP TS 23.218 [5] criteria based on the public user identity of the served user and start the evaluation of that iFC as described in subclause 5.4.3.2 starting at step 4B of subclause 5.4.3.2;

NOTE 4: The S-CSCF assesses triggering of services for the originating services after retargeting means it evaluates iFCs with a SessionCase set to ORIGINATING\_CDIV, as defined in 3GPP TS 29.228 [14]. If the P-Served-User extension specified in RFC 5502 [133] is supported, the S-CSCF uses the "orig-cdiv" header field parameter defined in draft-ietf-sipcore-originating-cdiv-parameter [239].

NOTE 5: The identity of the served user can be obtained from the History-Info header field (see RFC 4244 [66]) or the P-Served User header field as specified in RFC 5502 [133]. The served user can be a public user identity, a public GRUU, or a temporary GRUU. It needs to be ensure, that all ASs in the iFC can determine the served user correctly.

NOTE 6: The S-CSCF determines whether to apply a) or b) based on information in the initial Filter Criteria.

- 3A) if the Request-URI is a GRUU, but is not valid as defined in subclause 5.4.7A.4, then return a 4xx response as specified in RFC 5627 [93];
- 3B) if the Request-URI contains a public GRUU and the saved value of the Request-URI is a temporary GRUU, then replace the Request-URI with the saved value of the Request-URI;
- 3C) if the request contains a P-Asserted-Service header field check whether the IMS communication service identified by the ICSI value contained in the P-Asserted-Service header field is allowed by the subscribed services for the served user:
- a) if so, continue from step 4; and
  - b) if not, as an operator option, the S-CSCF may reject the request by generating a 403 (Forbidden) response. Otherwise, remove the P-Asserted-Service header field and continue with the rest of the steps;
- 3D) if the request does not contain a P-Asserted-Service header field check if the contents of the request matches a subscribed service (e.g. SDP media capabilities, Content-Type header field) for each and any of the subscribed services for the served user:
- a) if not, as an operator option, the S-CSCF may reject the request by generating a 403 (Forbidden) response. Otherwise, continue with the rest of the steps; and
  - b) if so, and if the request is related to an IMS communication service and the IMS communication service requires the use of an ICSI value then include a P-Asserted-Service header field in the request containing the ICSI value for the related IMS communication service, and use it as a header field in the initial request when matching initial filter criteria in step 4; and
  - c) if so, and if the request is related to an IMS communication service and the IMS communication service does not require the use of an ICSI value then continue without including an ICSI value; and
  - d) if so, and if the request does not relate to an IMS communication service (or if the S-CSCF is unable to unambiguously determine the service being requested but decides to allow the session to continue) then continue without including an ICSI value;
- 4) check whether the initial request matches any unexecuted initial filter criteria based on the public user identity of the served user in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then the S-CSCF shall select the first matching unexecuted initial filter criteria and:
- a) if the Request-URI is a temporary GRUU as defined in subclause 5.4.7A.3, then replace the Request-URI with the public GRUU that is associated with the temporary GRUU (i.e. the public GRUU representing the same public user identity and instance ID as the temporary GRUU);
  - b) insert the AS URI to be contacted into the Route header field as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;
  - c) if the S-CSCF supports the P-Served-User extension as specified in RFC 5502 [133], insert the P-Served-User header field populated with the served user identity as determined in step 1. If required by operator policy, the S-CSCF shall:
    - if the associated session case is "Terminating" as specified in 3GPP TS 29.228 [14], include the sescase header field parameter set to "term" and the regstate header field parameter set to "reg";
    - if the associated session case is "Terminating\_Unregistered" as specified in 3GPP TS 29.228 [14], include the sescase header field parameter set to "term" and the regstate header field parameter set to "unreg"; and
  - d) insert a type 3 "orig-ioi" header field parameter replacing any received "orig-ioi" header field parameter in the P-Charging-Vector header field. The type 3 "orig-ioi" header field parameter identifies the sending network of the request message. The S-CSCF shall not include the type 3 "term-ioi" header field parameter;

NOTE 7: Depending on the result of the previous process, the S-CSCF can contact one or more AS(s) before processing the outgoing Request-URI.

NOTE 8: If the Request-URI of the received terminating request contains a temporary GRUU, then step 4 replaces the Request-URI with the associated public GRUU before invoking the AS, and step 3B restores the original temporary GRUU when the request is returned from the AS.

NOTE 9: An AS can activate or deactivate its own filter criteria via the Sh interface. As the S-CSCF checks initial filter criteria only on receipt of an initial request for a dialog, or a standalone transaction, a modified service profile will have no impact on transactions or dialogs already in progress and the modified profile will be effective only for new transactions and dialogs. If the S-CSCF receives a modification of the iFC during their execution, then it should not update the stored initial Filter Criteria until the iFC related to the initial request have been completely executed.

- 5) if there was no original dialog identifier present in the topmost Route header field of the incoming request insert a P-Charging-Function-Addresses header field, if not present, populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;
- 6) if there was no original dialog identifier present in the topmost Route header field of the incoming request store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field and retain the "icid-value" header field parameter in the P-Charging-Vector header field;
- 7) if there was no original dialog identifier present in the topmost Route header field of the incoming request store the value of the "orig-ioi" header field parameter received in the P-Charging-Vector header field, if present, and remove received "orig-ioi", "term-ioi" and "transit-ioi" header field parameters from the forwarded request if next hop is not an AS;

NOTE 10: Any received "orig-ioi" header field parameter will be a type 2 IOI. or type 3 IOI. A type 2 IOI identifies the sending network of the request message, a type 3 IOI identifies the sending service provider of the request message.

- 7A) if there was an original dialog identifier present in the topmost Route header field of the incoming request store the value of the "orig-ioi" header field parameter received in the P-Charging-Vector header field, if present, and remove the received "orig-ioi" header field parameter if next hop is not an AS;

NOTE 11: Any received "orig-ioi" header field parameter will be a type 3 IOI. A type 3 IOI identifies the sending service provider of the request message.

- 8) in the case:
  - i) there are no Route header fields in the request; and
  - ii) there are bindings saved during registration or re-registration as described in subclause 5.4.1.2 which are not marked as created by an emergency registration as described in subclause 5.4.8.2;

then, create a target set of potential routes from the the list of preloaded routes associated with the bindings in item 8) ii), as follows:

- a) if the Request-URI contains a valid GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.4 that does not contain a "bnc" URI parameter, then the target set is determined by following the procedures for Request Targeting specified in RFC 5627 [93], using the public user identity and instance ID derived from the GRUU using the procedures of subclause 5.4.7A;
- b) if the Request-URI contains a valid public GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.4 that contains a "bnc" URI parameter then the target set is determined by following the procedures for routing of public GRUUs specified in RFC 6140 [191].

NOTE 12: The procedures for Request Targeting for public GRUUs in subclause 7.1.1 of RFC 6140 [191] involve copying the "sg" SIP URI parameter from the Public GRUU into the Request-URI along with the bound registered Contact Address.

NOTE 13: In this release of the specification, use of preloaded routes saved during registration or re-registration which created or refreshed bindings marked as created by an emergency registration is out of scope.

- c) if the Request-URI contains a temporary GRUU not assigned by the S-CSCF but that contains "temp-gruu-cookie" information provided by the S-CSCF to the UE in a "temp-gruu-cookie" header field parameter as specified in RFC 6140 [191] then the target set is determined by following the procedures for Request Targeting for temporary GRUUs specified in RFC 6140 [191]; or

NOTE 14: The procedures for obtaining the "temp-gruu-cookie" information from the temporary GRUU and for routing of temporary GRUUs are specified in subclause 7.1.2.3 of RFC 6140 [191].



- d) if the Request-URI contains a public user identity or a GRUU not assigned by the S-CSCF, then the target set is all the registered contacts saved for the destination public user identity;
- 9) if necessary perform the caller preferences to callee capabilities matching according to RFC 3841 [56B] to the target set;

NOTE 15: This might eliminate entries and reorder the target set.

NOTE 16: The S-CSCF performs caller preferences to callee capabilities matching also to select among multiple targets set to a single instance-id, when the UE has registered multiple registration flows.

10) in case there are no Route header fields in the request:

- a) if there is more than one route in the target set determined in steps 8) and 9) above:
- if the fork directive in the Request-Disposition header field was set to "no-fork", use the contact with the highest qvalue parameter to build the target URI. In case no qvalue parameters were provided, the S-CSCF shall decide locally what contact address to be used to build the target URI;
  - if the fork directive in the Request-Disposition header field was not set to "no-fork", fork the request or perform sequential search based on the relative preference indicated by the qvalue parameter of the Contact header field in the REGISTER request, as described in RFC 3261 [26]. In case no qvalue parameters were provided, then the S-CSCF determine the contact address to be used to build the target URI as directed by the Request-Disposition header field as described in RFC 3841 [56B]. If the Request-Disposition header field is not present, the S-CSCF shall decide locally whether to fork or perform sequential search among the contact addresses;
  - in case that no route is chosen, return a 480 (Temporarily unavailable) response or another appropriate unsuccessful SIP response and terminate these procedures; and
  - per the rules defined in RFC 5626 [92], the S-CSCF shall not populate the target set with more than one contact with the same public user identity and instance-id at a time. If a request for a particular public user identity and instance-id fails with a 430 response, the S-CSCF shall replace the failed branch with another target with the same public user identity and instance-id, but a different reg-id;
- b) If no "loose route" indication has been received, in the service profile of the served public user identity, from the HSS during registration, build the Request-URI with the contents of the target URI determined in the previous step, otherwise the Request-URI is retained as received;
- c) insert a P-Called-Party-ID SIP header field containing the contents of the Request-URI (if no "loose route" indication has been received, in the service profile of the served public user identity, from the HSS during registration, then exclude "rn" tel-URI parameter and "npdi" tel-URI parameter as defined in RFC 4694 [112]) received in the request unless the Request-URI contains a temporary GRUU in which case insert the public GRUU in the P-Called-Party-ID;
- d) build the Route header field with the Path values from the chosen route and if "loose route" indication has been received, in the service profile of the served user identity, from the HSS during registration and the selected contact address was not registered as described in RFC 5626 [92], add the content of the target URI determined in step a), as last URI of the route. If the selected contact address was registered as described in RFC 5626 [92], the target URI determined in step a) is not added to the Route header field; and
- e) save the Request-URI and the total number of Record-Route header fields as part of the dialog request state.

NOTE 17: For each initial dialog request terminated at a served user two pieces of state are maintained to assist in processing GRUUs: the chosen contact address to which the request is routed; and the position of an entry for the S-CSCF in the Record-Route header field that will be responsible for GRUU translation, if needed (the position is the number of entries in the list before the entry was added). The entry will be added in step 5) of the below procedures for handling S-CSCF receipt any 1xx or 2xx response to the initial request for a dialog. The S-CSCF can record-route multiple times, but only one of those (the last) will be responsible for gruu translation at the terminating end.

11) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;

12) optionally, apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header field and privacy required by RFC 4244 [66]. The S-CSCF shall not remove any priv-value from the Privacy header field;

NOTE 18: keeping the priv-value in the Privacy header field is necessary to indicate to the UE that the public user identity was not sent because of restriction. Although RFC 3323 [33] states that when a privacy service performs one of the functions corresponding to a privacy level listed in the Privacy header field, it SHOULD remove the corresponding priv-value from the Privacy header field, there is no harm that the S-CSCF does not remove the priv-values as there will be no other entity that would perform the privacy service after the S-CSCF.

NOTE 19: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

13) in case of an initial request for a dialog, either:

- if the request is routed to an AS which is part of the trust domain, the S-CSCF shall decide, based on operator policy, whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header field containing its own SIP URI; or
- if the request is routed elsewhere, create a Record-Route header field containing its own SIP URI;

13A) if the request is routed to the P-CSCF remove the P-User-Database header field and P-Served-User header field if present; and

14) forward the request based on the topmost Route header field.

If the S-CSCF:

- a) fails to receive a SIP response within a configurable time; or
- b) receives a 408 (Request Timeout) response or a 5xx response from the AS without previously receiving a 1xx response to the original SIP request, and without previously receiving a SIP request from the AS that contained the same original dialog identifier as the original request;

the S-CSCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION\_CONTINUED" as specified in 3GPP TS 29.228 [14] or no default handling is indicated, execute the procedure from step 4; and
- if the default handling defined in the filter criteria indicates the value "SESSION\_TERMINATED" as specified in 3GPP TS 29.228 [14], either forward the received response or, if the request is an initial INVITE request, send a 408 (Request Timeout) response or a 5xx response towards the originating UE as appropriate (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

If the S-CSCF receives any final response from the AS, the S-CSCF shall forward the response towards the originating UE (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

When the S-CSCF receives any response to the above request and forwards it to AS, the S-CSCF shall insert a P-Charging-Vector header field containing the "orig-ioi" header field parameter, if received in the request, and a type 3 "term-ioi" header field parameter in the response. The S-CSCF shall set the type 3 "term-ioi" header field parameter to a value that identifies the sending network of the response and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter.

NOTE 20: Any received "term-ioi" header field parameter will be a type 3 IOI. The type 3 IOI identifies the service provider from which the response was sent.

When the S-CSCF receives, destined for an unregistered served user or a statically pre-configured PSI, an initial request for a dialog or a request for a standalone transaction, the S-CSCF shall:

- 1) Void.
- 2) execute the procedures described in 1, 2, 3, 3C, 3D, 4, 5, 6, 7, 11, 13, 13B, 13C and 14 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

- 3) In case that no more AS needs to be contacted, then S-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) and terminate these procedures.

NOTE 21: When the S-CSCF does not have the user profile, before executing the actions as listed above, it initiates the S-CSCF Registration/deregistration notification procedure, as described in 3GPP TS 29.228 [14]; with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informs the HSS that the user is unregistered. The S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14]. When requesting the user profile the S-CSCF can include the information in the P-Profile-Key header field in S-CSCF Registration/deregistration notification. When requesting the user profile, and the request received by the S-CSCF contains a P-Profile-Key header field, the S-CSCF can include the header field value in S-CSCF Registration/deregistration notification. If the response from the HSS includes a Wildcarded Public Identity AVP, and if the request received by the S-CSCF did not include a P-Profile-Key header field, the S-CSCF uses the AVP value to set the P-Profile-Key header field before forwarding the request to an AS.

Prior to performing S-CSCF Registration/Deregistration procedure with the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14] or use the value as received in the P-User-Database header field in the initial request for a dialog or a request for a standalone transaction as defined in RFC 4457 [82]. The HSS address received in the response to SLF query can be used to address the HSS of the public user identity with further queries.

If the HSS indicates to the S-CSCF that there is already another S-CSCF assigned for the user, the S-CSCF shall return a 305 (Use Proxy) response containing the SIP URI of the assigned S-CSCF received from the HSS in the Contact header field.

When the S-CSCF receives any 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), the S-CSCF shall:

- 1) if the response corresponds to an INVITE request, save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed;
- 2) if the response is not forwarded to an AS (i.e. the response is related to a request that was matched to the first executed initial filter criteria), insert a type 2 "term-ioi" header field parameter in the P-Charging-Vector header field of the outgoing response. The type 2 "term-ioi" header field is set to a value that identifies the sending network of the response and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter. Values of "orig-ioi" and "term-ioi" header field parameters in the received response are removed;
- 3) in case the served user is not considered a privileged sender then:
  - a) if the P-Asserted-Identity header field contains only a SIP URI and in the case where the S-CSCF has knowledge that the SIP URI contained in the received P-Asserted-Identity header field is an alias SIP URI for a tel URI, the S-CSCF shall add a second P-Asserted-Identity header field containing this tel URI, including the display name associated with the tel URI, if available; and
  - b) if the P-Asserted-Identity header field contains only a tel URI, the S-CSCF shall add a second P-Asserted-Identity header field containing a SIP URI. The added SIP URI shall contain in the user part a "+" followed by the international public telecommunication number contained in tel URI, and user's home domain name in the hostport part. The added SIP URI shall contain the same value in the display name as contained in the tel URI. The S-CSCF shall also add a "user" SIP URI parameter equals "phone" to the SIP URI;
- 4) in case the response is sent towards the originating user, the S-CSCF may retain the P-Access-Network-Info header field based on local policy rules and the destination user (Request-URI);
- 5) save an indication that GRUU routing is to be performed for subsequent requests sent within this same dialog if:
  - a) there is a record-route position saved as part of the initial dialog request state; and
  - b) the contact address in the response is a valid GRUU assigned by the S-CSCF as specified in subclause 5.4.7A.4 or a temporary GRUU self assigned by the UE based on the "temp-gruu-cookie" header field parameter provided to the UE; and

NOTE 22: There could be several responses returned for a single request, and the decision to insert or modify the Record-Route needs to be applied to each. But a response might also return to the S-CSCF multiple times as it is routed back through AS. The S-CSCF will take this into account when carrying out step 5) to ensure that the information is stored only once.

- 6) if the response is forwarded within the S-CSCF home network and not to an AS, insert a P-Charging-Function-Addresses header field populated with values received from the HSS.

When the S-CSCF receives a response to a request for a standalone transaction (whether the user is registered or not), then:

- 1) in case the served user is not considered a privileged sender then:
  - a) if the P-Asserted-Identity header field contains only a SIP URI and in the case where the S-CSCF has knowledge that the SIP URI contained in the received P-Asserted-Identity header field is an alias SIP URI for a tel URI, the S-CSCF shall add a second P-Asserted-Identity header field containing this tel URI, including the display name associated with the tel URI, if available; and
  - b) if the P-Asserted-Identity header field contains only a tel URI, the S-CSCF shall add a second P-Asserted-Identity header field containing a SIP URI. The added SIP URI shall contain in the user part a "+" followed by the international public telecommunication number contained in tel URI, and user's home domain name in the hostport part. The added SIP URI shall contain the same value in the display name as contained in the tel URI. The S-CSCF shall also add a "user" SIP URI parameter equals "phone" to the SIP URI; and
- 2) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header field; otherwise, the S-CSCF shall remove the access-network-charging-info parameter in the P-Charging-Vector header field.

When the S-CSCF receives the 200 (OK) response for a standalone transaction request, the S-CSCF shall:

- 1) insert a P-Charging-Function-Addresses header field populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards an AS; and
- 2) if the response is not forwarded to an AS (i.e. the response is related to a request that was matched to the first executed initial filter criteria), insert a type 2 "term-ioi" header field parameter in the P-Charging-Vector header field of the outgoing response. The type 2 "term-ioi" header field parameter is set to a value that identifies the sending network of the response and the type 2 "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter.

NOTE 23: If the S-CSCF forked the request of a stand alone transaction to multiple UEs and receives multiple 200 (OK) responses, the S-CSCF will select and return only one 200 (OK) response. The criteria that the S-CSCF employs when selecting the 200 (OK) response is based on the operator's policy (e.g. return the first 200 (OK) response that was received).

When the S-CSCF receives, destined for a served user, a target refresh request for a dialog, prior to forwarding the request, the S-CSCF shall:

- 0) if the dialog is related to an IMS communication service determine whether the contents of the request (e.g. SDP media capabilities, Content-Type header field) match the IMS communication service as received as the ICSI value in the P-Asserted-Service header field in the initial request. As an operator option, if the contents of the request do not match the IMS communication service the S-CSCF may reject the request by generating a status code reflecting which added contents are not matching. Otherwise, continue with the rest of the steps;
- 1) if the incoming request is received on a dialog for which GRUU routing is to be performed and the Request-URI is not the GRUU for this dialog, then return a response of 400 (Bad Request).
- 2) if the incoming request is received on a dialog for which GRUU routing is to be performed and the Request-URI contains the GRUU for this dialog then:
  - i) if the Request-URI contains a valid GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.4 that does not contain a "bnc" URI parameter, then perform the procedures for Request Targeting specified in RFC 5627 [93], using the public user identity and instance ID derived from the Request-URI, as specified in subclause 5.4.7A;

- ii) if the Request-URI contains a valid public GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.4 that contains a "bnc" URI parameter then the target set is determined by following the procedures for routing of public GRUUs specified in RFC 6140 [191]. or

NOTE 24: The procedures for Request Targeting for public GRUUs in subclause 7.1.1 of RFC 6140 [191] involve copying the "sg" SIP URI parameter from the Public GRUU into the Request-URI along with the bound registered Contact Address.

- iii) if the Request-URI contains a temporary GRUU not assigned by the S-CSCF but that contains "temp-gruu-cookie" information provided by the S-CSCF to the UE in a "temp-gruu-cookie" header field parameter as specified in RFC 6140 [191] then the target set is determined by following the procedures for routing of temporary GRUUs specified in RFC 6140 [191];

NOTE 25: The procedures for obtaining the "temp-gruu-cookie" information from the temporary GRUU and for routing of temporary GRUUs are specified in subclause 7.1.2.3 of RFC 6140 [191].

- iv) if no contact can be selected, return a response of 480 (Temporarily Unavailable);
- 3) remove its own URI from the topmost Route header field;
- 4) for INVITE dialogs (i.e. dialogs initiated by an INVITE request), save the Contact and CSeq header field values received in the request such that the S-CSCF is able to release the session if needed;
- 5) create a Record-Route header field containing its own SIP URI; and
- 6) forward the request based on the topmost Route header field.

When the S-CSCF receives any 1xx or 2xx response to the target refresh request for a dialog (whether the user is registered or not), the S-CSCF shall:

- 1) for INVITE dialogs, replace the saved Contact header field values in the response such that the S-CSCF is able to release the session if needed; and
- 2) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header field; otherwise, the S-CSCF shall remove the access-network-charging-info parameter in the P-Charging-Vector header field.

When the S-CSCF receives, destined for the served user, a subsequent request other than target refresh request for a dialog, prior to forwarding the request, the S-CSCF shall:

- 1) if the incoming request is received on a dialog for which GRUU routing is to be performed and the Request-URI is not the GRUU for this dialog, then return a response of 400 (Bad Request).
- 2) if the incoming request is received on a dialog for which GRUU routing is to be performed and the Request-URI contains the GRUU for this dialog then:
  - i) if the Request-URI contains a valid GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.4 that does not contain a "bnc" URI parameter, then perform the procedures for Request Targeting specified in RFC 5627 [93], using the public user identity and instance ID derived from the Request-URI, as specified in subclause 5.4.7A;
  - ii) if the Request-URI contains a valid public GRUU assigned by the S-CSCF as defined in subclause 5.4.7A.4 that contains a "bnc" URI parameter then the target set is determined by following the procedures for routing of public GRUUs specified in RFC 6140 [191]; or

NOTE 26: The procedures for Request Targeting for public GRUUs in subclause 7.1.1 of RFC 6140 [191] involve copying the "sg" SIP URI parameter from the Public GRUU into the Request-URI along with the bound registered Contact Address.

- iii) if the Request-URI contains a temporary GRUU not assigned by the S-CSCF but that contains "temp-gruu-cookie" information provided by the S-CSCF to the UE in a "temp-gruu-cookie" header field parameter as specified in RFC 6140 [191] then the target set is determined by following the procedures for routing of temporary GRUUs specified in RFC 6140 [191].

NOTE 27: The procedures for obtaining the "temp-gruu-cookie" information from the temporary GRUU and for routing of temporary GRUUs are specified in subclause 7.1.2.3 of RFC 6140 [191].

- iv) if no contact can be selected, return a response of 480 (Temporarily Unavailable).
- 3) remove its own URI from the topmost Route header field; and
- 4) forward the request based on the topmost Route header field.

When the S-CSCF receives a response to a subsequent request other than target refresh request for a dialog, in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the access-network-charging-info parameter from the P-Charging-Vector header field; otherwise, the S-CSCF shall remove the access-network-charging-info parameter from the P-Charging-Vector header field.

With the exception of 305 (Use Proxy) responses, the S-CSCF shall not recurse on 3xx responses.

#### 5.4.3.4 Original dialog identifier

The original dialog identifier is an implementation specific token that the S-CSCF encodes into the own S-CSCF URI in a Route header field, prior to forwarding the request to an AS. This is possible because the S-CSCF is the only entity that creates and consumes the value.

The token may identify the original dialog of the request, so in case an AS acting as a B2BUA changes the dialog, the S-CSCF is able to identify the original dialog when the request returns to the S-CSCF. In a case of a standalone transaction, the token indicates that the request has been sent to the S-CSCF from an AS in response to a previously sent request. The token can be encoded in different ways, such as e.g., a character string in the user-part of the S-CSCF URI, a parameter in the S-CSCF URI or port number in the S-CSCF URI.

The S-CSCF shall ensure that the value chosen is unique so that the S-CSCF may recognize the value when received in a subsequent message of one or more dialogs and make the proper association between related dialogs that pass through an AS.

An original dialog identifier is sent to each AS invoked due to iFC evaluation such that the S-CSCF can associate requests as part of the same sequence that trigger iFC evaluation in priority order (and not rely on SIP dialog information that may change due to B2BUA AS).

**NOTE:** If the same original dialog identifier is included in more than one request from a particular AS (based on service logic in the AS), then the S-CSCF will continue the iFC evaluation sequence. If the AS wants iFC evaluation to start from the beginning for a request, then AS should not include an original dialog identifier;

#### 5.4.3.5 Void

#### 5.4.3.6 SIP digest authentication procedures for all SIP request methods initiated by the UE excluding REGISTER

##### 5.4.3.6.1 General

When the S-CSCF receives from the UE a request (excluding REGISTER), and SIP digest without TLS or SIP digest with TLS is supported and in use for this UE, the S-CSCF may perform the following steps if authentication of SIP request methods initiated by the UE excluding REGISTER is desired:

- 1) The S-CSCF shall identify the user by the public user identity as received in the P-Asserted-Identity header field;
- 2) If the public user identity does not match one of the registered public user identities, and the public user identity does not match one of the registered wildcarded public user identities, the S-CSCF may reject the request with a 400 (Bad Request) response or silently discard the request;
- 3) If the request does not contain a Proxy-Authorization header field or the Proxy-Authorization header field does not contain a digest response, the S-CSCF shall:
  - a) challenge the user by generating a 407 (Proxy Authentication Required) response for the received request, including a Proxy-Authenticate header field as defined in RFC 2617 [21], which includes:
    - a "realm" header field parameter;
    - a "nonce" header field parameter, with a newly generated value by the S-CSCF;

- an "algorithm" header field parameter; if the algorithm value is not provided in the authentication vector, it shall have the value "MD5"; and
- a "qop" header field parameter; if the qop value is not provided in the authentication vector, it shall have the value "auth".

The challenge parameters, with the exception of the "nonce" header field parameter, shall be the same as the ones used for the last successful registration.

NOTE: The usage of the same parameters for authentication of non-registration SIP requests requires the storage of these parameters during authentication of REGISTER requests, as retrieval of authentication vectors is only specified for REGISTER requests.

- b) send the so generated 407 (Proxy Authentication Required) response towards the UE; and,
  - c) retain the nonce and initialize the corresponding nonce count to a value of 1.
- 4) If the request contains a Proxy-Authorization header field, the S-CSCF shall:
- a) check whether the Proxy-Authorization header field contains:
    - the private user identity of the user in the "username" header field parameter;
    - an "algorithm" header field parameter value which matches the "algorithm" header field parameter in the authentication challenge (i.e. "MD5");
    - a "response" header field parameter with the authentication challenge response;
    - a "realm" header field parameter matching the "realm" header field parameter in the authentication challenge;
    - "nonce" header field parameter matching the expected nonce from either a recent authentication challenge or a more recent "nextnonce" header field parameter sent in a Proxy-Authentication-Info header field;
    - a "uri" header field parameter matching the SIP Request-URI;
    - a "cnonce" header field parameter; and
    - a "nonce-count" header field parameter with a value that equals the nonce-count expected by the S-CSCF. The S-CSCF may choose to accept a nonce-count which is greater than the expected nonce-count. If the S-CSCF uses this nonce-count and authentication is successful and the S-CSCF increments it for any subsequent authentication responses.

If any of the above checks do not succeed, the S-CSCF shall proceed as described in subclause 5.4.3.6.2, and skip the remainder of this procedure.

- b) check whether the received authentication challenge response and the expected authentication challenge response match. The S-CSCF shall compute the expected digest response as described in RFC 2617 [21] using the H(A1) value contained within the authentication vector, and other digest parameters (i.e. nonce, cnonce, nonce-count, qop).

In the case where the digest response does not match the expected digest response calculated by the S-CSCF, the S-CSCF shall consider the authentication attempt as failed and do one of the following:

- 1) rechallenge the user by issuing a 407 (Proxy Authentication Required) response including a challenge as per procedures described in this subclause; or
- 2) reject the request by issuing a 403 (Forbidden) response; or
- 3) reject the request without sending a response.

In the case where the digest response matches the expected digest response calculated by the S-CSCF, the S-CSCF shall consider the identity of the user verified and the request authenticated and continue with the procedures as described in subclause 5.4.3.

### 5.4.3.6.2 Abnormal cases

In the case that SIP digest is used and the request from the UE contains an invalid "nonce" Authorization header field parameter with a valid challenge response for that nonce (indicating that the client knows the correct username/password), or when the "nonce-count" Authorization header field parameter value sent by the UE is not the expected value, or when the Proxy-Authorization header field does not include the correct parameters, the S-CSCF shall:

- send a 407 (Proxy Authentication Required) response to initiate a further authentication attempt with a fresh nonce and the "stale" header field parameter set to "true" in the Proxy-Authenticate header field.

When the S-CSCF cannot forward an initial incoming request to an Application Server due to overload control mechanism, it shall either

- if the default handling defined in the filter criteria indicates the value "SESSION\_CONTINUED" as specified in 3GPP TS 29.228 [14] or no default handling is indicated, execute the procedure from step 5 in subclause 5.4.3.2 or from step 4 in subclause 5.4.3.3 depending on the type of request; and
- if the default handling defined in the filter criteria indicates the value "SESSION\_TERMINATED" as specified in 3GPP TS 29.228 [14], reject the request as specified in RFC 7339 [199] and RFC 7200 [201] (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

## 5.4.4 Call initiation

### 5.4.4.1 Initial INVITE

When the S-CSCF receives an INVITE request, either from the served user or destined to the served user, the S-CSCF may require the periodic refreshment of the session to avoid hung states in the S-CSCF. If the S-CSCF requires the session to be refreshed, the S-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

For interworking with a visiting network, where the P-CSCF of the visiting network does not support priority but it is intended or required to give users of that P-CSCF priority in the home network, the S-CSCF in the home network shall recognize the need for priority treatment if such detection is not alternately provided via an IBCF in the home network.

NOTE 2: Various mechanisms can be applied to recognize the need for priority treatment (e.g., based on the dialled digits). The exact mechanisms are left to national regulation and network configuration.

When an S-CSCF interworks with a visiting network that does not support priority, and the S-CSCF recognizes the need for priority treatment, the S-CSCF shall insert the temporarily authorised Resource-Priority header field with appropriate namespace and priority value in the INVITE request.

When the S-CSCF receives an initial INVITE request destined for the served user, the S-CSCF shall either:

- a) examine the SDP offer (the "c=" parameter) to detect if it contains an IP address type that is not supported by the IM CN subsystem; or

NOTE 3: The S-CSCF can, based on local policy, assume that a UE supports the IP address type of the SDP offer for media if it is identical to the address type of a contact that the UE has registered.

- b) process the initial INVITE request without examining the SDP.

NOTE 4: If the S-CSCF knows that the terminating UE supports both IPv6 and IPv4 addressing simultaneously, the S-CSCF will forward the initial INVITE request to the UE without examining the SDP. The present version of the specification does not specify how the S-CSCF determines whether the UE supports both IPv6 and IPv4 addressing simultaneously.

NOTE 5: If the SDP offer contained an IP address type that is not supported by the IM CN subsystem, the S-CSCF will receive the 488 (Not Acceptable Here) response with 301 Warning header field indicating "incompatible network address format".

Subsequently, when the S-CSCF detects that the SDP offer contained an IP address type that is not supported by the IM CN subsystem (i.e., either case a) or b)), the S-CSCF shall either:



- return a 305 (Use Proxy) response to the I-CSCF with the Contact field containing the SIP URI of the IBCF, or
- forward the initial INVITE request to the IBCF. When forwarding the initial INVITE request, the S-CSCF shall not insert its SIP URI into the Record-Route header field.

If overlap signalling using the multiple-INVITE method is supported as a network option, several INVITE requests with the same Call ID and the same From header field (including "tag" header field parameter) can be received outside of an existing dialog. Such INVITE requests relate to the same call. If the S-CSCF receives an INVITE request from the served user outside an existing dialog with the same Call ID and From header field as a previous INVITE request during a certain period of time, it shall route the new INVITE request to the same next hop as the previous INVITE request.

## 5.4.4.2 Subsequent requests

### 5.4.4.2.1 UE-originating case

When the S-CSCF receives the request containing the access-network-charging-info parameter in the P-Charging-Vector, the S-CSCF shall store the access-network-charging-info parameter from the P-Charging-Vector header field. The S-CSCF shall retain access-network-charging-info parameter in the P-Charging-Vector header field when the request is forwarded to an AS. However, the S-CSCF shall not include the access-network-charging-info parameter in the P-Charging-Vector header field when the request is forwarded outside the home network of the S-CSCF.

When the S-CSCF receives any request or response (excluding ACK requests and CANCEL requests and responses) related to a UE-originated dialog or standalone transaction, the S-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses header fields before forwarding the message within the S-CSCF home network, including towards AS.

### 5.4.4.2.2 UE-terminating case

When the S-CSCF receives 180 (Ringing) or 200 (OK) (to INVITE) responses containing the access-network-charging-info parameter in the P-Charging-Vector, the S-CSCF shall store the access-network-charging-info parameter from the P-Charging-Vector header field. The S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header field when the response is forwarded to an AS. However, the S-CSCF shall not include the access-network-charging-info parameter in the P-Charging-Vector header field when the response is forwarded outside the home network of the S-CSCF.

When the S-CSCF receives any request or response (excluding ACK requests and CANCEL requests and responses) related to a UE-terminated dialog or standalone transaction, the S-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses header fields before forwarding the message within the S-CSCF home network, including towards AS.

When the S-CSCF receives an error response (to INVITE) for an existing early dialog, and if the S-CSCF does not forward the response immediately (if the S-CSCF forked the INVITE request it may wait for additional final responses), the S-CSCF does not have knowledge of having received an 199 (Early Dialog Terminated) provisional response on the same early dialog, and the associated INVITE request included the "199" option-tag in the Supported header field, and the INVITE request did not include the "100rel" option tag in the Require header field, the S-CSCF shall trigger and send an unreliable 199 (Early Dialog Terminated) provisional response, using the same "tag" To header field parameter value as the error response, as specified in in RFC 6228 [142].

## 5.4.5 Call release

### 5.4.5.1 S-CSCF-initiated session release

#### 5.4.5.1.1 Cancellation of a session currently being established

Upon receipt of a network internal indication to release a session which is currently being established, the S-CSCF shall:

- 1) cancel the related dialogs by sending the CANCEL request according to the procedures described in RFC 3261 [26]; and
- 2) send an appropriate response to the sender of the original INVITE request.

#### 5.4.5.1.2 Release of an existing session

Upon receipt of a network internal indication to release an existing multimedia session, the S-CSCF shall:

- 1) if the S-CSCF serves the calling user of the session, generate a BYE request destined for the called user based on the information saved for the related dialog, including:
  - a Request-URI, set to the stored Contact header field provided by the called user;
  - a To header field, set to the To header field value as received in the 200 (OK) response for the initial INVITE request;
  - a From header field, set to the From header field value as received in the initial INVITE request;
  - a Call-ID header field, set to the Call-Id header field value as received in the initial INVITE request;
  - a CSeq header field, set to the CSeq value that was stored for the direction from the calling to the called user, incremented by one;
  - a Route header field, set to the routing information towards the called user as stored for the dialog;
  - a Reason header field that contains proper SIP response code;
  - further header fields, based on local policy;
  - treat the BYE request as if received directly from the calling user, i.e. the S-CSCF shall send the BYE request to the internal service control and based on the outcome further on towards the called user; and
- 2) if the S-CSCF serves the calling user of the session, generate an additional BYE request destined for the calling user based on the information saved for the related dialog, including:
  - a Request-URI, set to a contact address obtained from the stored Contact header field if provided by the calling user. If the stored Contact header field contained either a public or a temporary GRUU, the S-CSCF shall set the Request-URI either to:
    - a) the contact address bound to the respective GRUU, if the stored Contact header field did not include an "ob" SIP URI parameter; or
    - b) the contact address that the UE used to send the initial INVITE request, if the stored Contact header field included an "ob" SIP URI parameter;

NOTE 1: Since the same public GRUU can be bound to multiple contact addresses of the UE that were registered as specified in RFC 5626 [92], the S-CSCF selects the contact address that the UE used to send the initial INVITE request.

- a To header field, set to the From header field value as received in the initial INVITE request;
  - a From header field, set to the To header field value as received in the 200 (OK) response for the initial INVITE request;
  - a Call-ID header field, set to the Call-Id header field value as received in the initial INVITE request;
  - a CSeq header field, set to the CSeq value that was stored for the direction from the called to the calling user, incremented by one – if no CSeq value was stored for that session the S-CSCF shall generate and apply a random number within the valid range for CSeqs;
  - a Route header field, set to the routing information towards the calling user as stored for the dialog;
  - a Reason header field that contains proper SIP response code;
  - further header fields, based on local policy;
  - send the BYE request directly to the calling user.
- 3) if the S-CSCF serves the called user of the session, generate a BYE request destined for the called user based on the information saved for the related dialog, including:

- a Request-URI, set to a contact address that the S-CSCF uses to send the in-dialog requests towards the called UE as defined in RFC 5626 [92] and RFC 5627 [93];
  - a To header, set to the To header value as received in the 200 (OK) response for the initial INVITE request;
  - a From header, set to the From header value as received in the initial INVITE request;
  - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
  - a CSeq header, set to the CSeq value that was stored for the direction from the calling to the called user, incremented by one;
  - a Route header, set to the routing information towards the called user as stored for the dialog;
  - a Reason header that contains proper SIP response code;
  - further headers, based on local policy;
  - send the BYE request directly to the called user; and
- 4) if the S-CSCF serves the called user of the session, generate an additional BYE request destined for the calling user based on the information saved for the related dialog, including:
- a Request-URI, set to the stored Contact header field provided by the calling user;
  - a To header, set to the From header field value as received in the initial INVITE request;
  - a From header, set to the To header field value as received in the 200 (OK) response for the initial INVITE request;
  - a Call-ID header, set to the Call-Id header field value as received in the initial INVITE request;
  - a CSeq header, set to the CSeq value that was stored for the direction from the called to the calling user, incremented by one – if no CSeq value was stored for that session the BYE shall generate and apply a random number within the valid range for CSeqs;
  - a Route header field, set to the routing information towards the calling user as stored for the dialog;
  - a Reason header field that contains proper SIP response code;
  - further headers, based on local policy;
  - treat the BYE request as if received directly from the called user, i.e. the S-CSCF shall send the BYE request to the internal service control and based on the outcome further on towards the calling user..

Upon receipt of the 2xx responses for both BYE requests, the S-CSCF shall release all information related to the dialog and the related multimedia session.

#### 5.4.5.1.2A Release of the existing dialogs due to registration expiration

When:

- 1) the registration lifetime of the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered) and bound either to the contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used) expires;
- 2) there are still active multimedia sessions that includes either this user's contact address or the registration flow and the associated contact address (if the multiple registration mechanism is used);
- 3) the session was initiated by or terminated towards the user using the public user identity currently registered or with one of the implicitly registered public used identities bound either to the contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used);

then the S-CSCF shall:

- release each of these multimedia sessions by applying the steps listed in the subclause 5.4.5.1.2. The S-CSCF shall only release dialogs associated with the multi media sessions originated or terminated towards the registered user's contact address or the registration flow and the associated contact address (if the multiple registration mechanism is used).

#### 5.4.5.1.3 Abnormal cases

Upon receipt of a request on a dialog for which the S-CSCF initiated session release, the S-CSCF shall terminate the received request and answer it with a 481 (Call/Transaction Does Not Exist) response.

#### 5.4.5.2 Session release initiated by any other entity

Upon receipt of a 2xx response for a BYE request matching an existing dialog, the S-CSCF shall delete all the stored information related to the dialog.

#### 5.4.5.3 Session expiration

If the S-CSCF requested the session to be refreshed periodically, and the S-CSCF got the indication that the session will be refreshed, when the session timer expires, the S-CSCF shall delete all the stored information related to the dialog.

### 5.4.6 Call-related requests

#### 5.4.6.1 ReINVITE

##### 5.4.6.1.1 Determination of served user

Void.

##### 5.4.6.1.2 UE-originating case

For a reINVITE request or UPDATE request from the UE within the same dialog, the S-CSCF shall store the updated access-network-charging-info parameter from P-Charging-Vector header field in the received SIP request. The S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header field when the request is forwarded to an AS. However, the S-CSCF shall not include the access-network-charging-info parameter in the P-Charging-Vector header field when the request is forwarded outside the home network of the S-CSCF.

For a reINVITE request from the UE, if the request is to be forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the access-network-charging-info parameter from the P-Charging-Vector header field; otherwise, the S-CSCF shall remove the access-network-charging-info parameter from the P-Charging-Vector header field.

##### 5.4.6.1.3 UE-terminating case

For a reINVITE request or UPDATE request destined towards the UE within the same dialog, when the S-CSCF receives the 200 (OK) response (to the INVITE request or UPDATE request), the S-CSCF shall store the updated access-network-charging-info parameter from the P-Charging-Vector header field. The S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header field when the response is forwarded to the AS. However, the S-CSCF shall not include the access-network-charging-info parameter in the P-Charging-Vector header field when the 200 (OK) response is forwarded outside the home network of the S-CSCF.

For any SIP response to an INVITE request, if the response is to be forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the access-network-charging-info parameter from the P-Charging-Vector header field; otherwise, the S-CSCF shall remove the access-network-charging-info parameter from the P-Charging-Vector header field.

#### 5.4.7 Void

### 5.4.7A GRUU management

#### 5.4.7A.1 Overview of GRUU operation

The S-CSCF provides a service of assigning and translating GRUUs for use by registered UEs, unless "loose route" has been provisioned in the service profile of the registered public user identity. This is conducted as specified in RFC 5627 [93] and RFC 5628 [94]. Two kinds of GRUUs are assigned: public GRUUs and temporary GRUUs.

NOTE: If the UE performs the functions of an external attached network (e.g an enterprise network) the UE could have self allocated its own GRUUs. In this version of the specification only UE self allocated public GRUUs are supported. Routing to a specific UE self-allocated public GRUUs requires that "loose route" is provisioned in the service profile of the served public user identity. Use of UE self-allocated temporary GRUUs is not supported in this version of the specification and requests addressed to UE self allocated temporary GRUUs will fail to be routed to the UE.

Each assigned GRUU represents an association between a public user identity and an instance ID provided by a registering UE. It is used to address a particular UE that possesses the instance ID and registers with the public user identity. The GRUU also denotes a contact address registered with a public user identity when the contact address has a "+sip.instance" header field parameter containing the the GRUU instance ID.

The S-CSCF issues GRUUs as part of the registration process, and also reports GRUUs as part of notifications for subscriptions to the "reg" event package. The S-CSCF always issues GRUUs in pairs – a public GRUU and a temporary GRUU. In case of implicit registration the S-CSCF assigns a unique public GRUU and a unique temporary GRUU for each public user identity.

The S-CSCF may also support the procedures for allocating public GRUUs and supporting the generation of temporary GRUUs by the functionality within the UE that performs the role of registrar as specified in RFC 6140 [191] as well as the procedures to route requests containing such GRUUs.

#### 5.4.7A.2 Representation of public GRUUs

Each public GRUU shall conform to all requirements specified in RFC 5627 [93].

If the Contact URI in the Contact header field does not contain a "bnc" URI parameter, then the S-CSCF constructs a public GRUU by adding a "gr" SIP URI parameter to the canonical form of the SIP URI which contains a public user identity.

If the Contact URI in the Contact header field contains a "bnc" URI parameter and if the S-CSCF supports RFC 6140 [191], then the S-CSCF constructs a public GRUU by adding both "bnc" and "gr" SIP URI parameters to the canonical form of the SIP URI from the To header field of the REGISTER request

The public GRUU that is returned in the "pub-gruu" parameter in the 200 (OK) response to the REGISTER request is constructed using the canonical form of the SIP URI of the public user identity from the To header field of the REGISTER request provided that public user identity is not barred. If the public user identity from the To header field of the REGISTER request is barred then the public GRUU that is returned in the "pub-gruu" parameter in the 200 (OK) response to the REGISTER request is constructed using the canonical form of the SIP URI of the default public user identity.

NOTE 1: The default public user identity is always provisioned as a SIP URI.

The "gr" SIP URI parameter serves as an indicator that the URI is in fact a GRUU and if the "+sip.instance" header field parameter from the Contact address contains an IMEI URN or a MEID URN then it carries a value that encodes the IMEI based instance ID that is defined in 3GPP TS 23.003 [3] or the MEID based instance ID which is defined in RFC 8464 [187] otherwise it carries the value received in the "+sip.instance" header field parameter.

By default, the value of the "gr" SIP URI parameter is a copy of the value of the "+sip.instance" header field parameter from a Contact address registered with the S-CSCF, with escaping of special characters as specified in RFC3261 [26].

If the "+sip.instance" header field parameter from the Contact address contains an IMEI URN, as specified in RFC 7254 [153] or an MEID URN, as specified in RFC 8464 [187], then the value of the "gr" SIP URI parameter is generated by the S-CSCF using the name-based UUID algorithm defined in RFC 4122 [154]. The following applies to the algorithm:

- 1) the "name space ID" shall be a UUID generated for use across the administrative domain and shall use the algorithm for creating a UUID from truly random numbers specified in RFC 4122 [154];

NOTE 2: If the generated UUID is changed, then newly created GRUUs will not match those that were created with the previous UUID. Therefore, the UUID needs to remain the same in order to create consistent GRUUs. This means that the namespace UUID needs to be the same for all S-CSCFs within the domain for which the public GRUU is hosted (it cannot be generated at run time by the S-CSCF as that would produce different values).

- 2) SHA-1 shall be used as the hash algorithm; and

- 3) the "name" is made up of a concatenation of the ASCII representation (see RFC 20 [212]) of:
- a) if IMEI, the TAC and SNR portions of the IMEI; or
  - b) if MEID, the Manufacturer Code and the Serial Number portions of the MEID;
- from the "+sip.instance" header field parameter.

Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks, and the S-CSCF shall follow the procedures for an IMEI as described above.

The S-CSCF shall store the "gr" parameter used in a public GRUU and the associated value received in a "+sip.instance" header field parameter.

The public GRUU for a particular association of public user identity and instance ID is persistent. The same public GRUU will be returned each time a registration is performed with a particular pair of public user identity and instance ID.

### 5.4.7A.3 Representation of temporary GRUUs

NOTE 1: For UEs performing the functions of an external attached network that support RFC 6140 [191] the S-CSCF does not allocate temporary GRUUs but assists the functionality within the UE that performs the role of registrar in allocating its own temporary GRUUs by providing to the UE the "temp-gruu-cookie" header field parameter that uniquely identifies the registration. The functionality within the UE that performs the role of registrar then is able to allocate its own temporary GRUUs as per RFC 6140 [191] procedures.

Each temporary GRUU shall conform to all requirements specified in RFC 5627 [93].

Because of the limited lifetime of a temporary GRUU, only the S-CSCF that created a temporary GRUU is required to understand how to translate that GRUU to the corresponding public user identity and instance ID.

The temporary GRUU that is returned in the "temp-gruu" parameter in the 200 (OK) response to the REGISTER request is mapped to the public user identity from the To header field of the REGISTER request provided that public user identity is not barred. If the public user identity from the To header field of the REGISTER request is barred then the temporary GRUU that is returned in the "temp-gruu" parameter in the 200 (OK) response to the REGISTER request is mapped to the default public user identity.

NOTE 2: The default public user identity is always provisioned as a SIP URI.

The specific representation of a temporary GRUU may be decided by each S-CSCF implementation. Temporary GRUUs must route to the assigning S-CSCF without requiring each assigned GRUU to be stored in the HSS.

The S-CSCF may choose a representation of temporary GRUUs that requires no extra state to be retained, such as that specified in RFC 5627 [93]. Alternatively, the S-CSCF may choose a stateful representation. This is an implementation choice.

NOTE 3: One possible implementation is for the S-CSCF to have a statically configured wildcard PSI that routes to it, with each temporary GRUU being encoded so that it matches the wildcard.

### 5.4.7A.4 GRUU recognition and validity

The S-CSCF shall recognize those GRUUs it has assigned, verify their validity, and extract the associated public user identity or stored identity of the UE that represents the functionality within the UE that performs the role of registrar and instance ID. This is true for both public GRUUs and temporary GRUUs.

NOTE 1: The S-CSCF only validates and extracts the associated public user identity and instance ID for GRUUs that it assigned.

GRUUs are distinguished from other URIs by the presence of a "gr" SIP URI parameter. Public GRUUs are distinguished from temporary GRUUs by the presence of a value for the "gr" SIP URI parameter.

The instance ID is obtained from a public GRUU by using the "gr" parameter to retrieve the stored associated instance ID. The public user identity or stored identity of the UE that represents the functionality within the UE that performs the role of registrar is extracted from a public GRUU by removing the "gr" SIP URI parameter.

The S-CSCF can recognize a public GRUU as valid if the "gr" parameter contains a value that was stored in the S-CSCF during generation of the public GRUU, and the derived public user identity compares equal, according to the comparison rules of RFC3261 [26], to a public user identity active within the S-CSCF or a stored identity of the UE that represents the functionality within the UE that performs the role of registrar from which a public GRUU was created. When validating public GRUUs the S-CSCF shall ignore the presence of any "sg" SIP URI parameter when determining if a public GRUU is one allocated by the S-CSCF.

NOTE 2: The UE that supports RFC 6140 [191] and performs the functions of an external attached network, adds a unique "sg" SIP URI parameter value to the public GRUU supplied by the S-CSCF when generating public GRUUs for its registering UAs.

The public user identity and instance ID are derived from a temporary GRUU via implementation specific means consistent with the way temporary GRUUs are constructed. The S-CSCF shall determine the validity of a temporary GRUU in conformance with RFC 5627 [93], and if the GRUU was allocated using RFC 6140 [191] procedures then in conformance with RFC 6140 [191] or using implementation specific means.

The S-CSCF regards a UE self-allocated public GRUU as valid if "loose route" is provisioned in the service profile of the served public user identity.

## 5.4.8 Emergency service

### 5.4.8.1 General

S-CSCF shall handle the emergency registration as per the needs of the normal registration.

NOTE: Emergency specific procedures for the Cx interface are specified in annex G in 3GPP TS 29.228 [14].

### 5.4.8.2 Initial emergency registration or user-initiated emergency reregistration

When the S-CSCF receives a REGISTER request; and the Contact header field includes a "sos" SIP URI parameter that indicates that this is an emergency registration, the S-CSCF shall perform the actions as specified in subclause 5.4.1.1 with the following additions:

- 1) when handling unprotected REGISTER request or protected REGISTER request, the S-CSCF:
  - a) shall deregister only contacts that were registered as part of emergency registration; and
  - b) shall not deregister contacts that were registered as part of non-emergency registration;

NOTE 1: other conditions triggering contact deregistration are described in subclause 5.4.1.

- 2) for the protected REGISTER request, when the S-CSCF receives a REGISTER request with the "integrity-protected" header field parameter in the Authorization header field set to "yes", "tls-yes" or "ip-assoc-yes", i.e. for the protected REGISTER request, and the Contact header field includes a "sos" SIP URI parameter that indicates that this is an emergency registration, the S-CSCF shall identify the user by the public user identity as received in the To header field and the private user identity as received in the Authorization header field of the REGISTER request;
- 3) if operator policy does not require that emergency service requests are forwarded to the S-CSCF, the S-CSCF shall not include a Service-Route header field in the 200 (OK) response to the REGISTER request;
- 4) the S-CSCF shall not include a temporary GRUU in the 200 (OK) response to the REGISTER request;
- 5) the S-CSCF shall include the "sos" URI parameter in the URI that was successfully emergency registered and included in the Contact header field of the 200 (OK) response to the REGISTER request;

NOTE 2: In the case where the S-CSCF returns a GRUU in the Contact header field of the 200 (OK) response to the REGISTER request, the "sos" URI parameter is appended to the URI and not included as a Contact header field parameter. The public GRUU that is returned in the 200 (OK) response includes the "sos" URI parameter as a parameter of the URI included in the "pub-gruu" Contact header field parameter.

- 6) store the Path header field and the contact information including all header field parameters contained in the Contact header field;

NOTE 3: The Path header field and contact information used for the emergency dialogs destined for the UE and obtained during the emergency registration can be different than the Path header field used for the non-emergency communication and obtained during the non-emergency registration.

NOTE 4: The S-CSCF will not perform the network initiated deregistration procedure for an emergency registration, but will let it expire. A new emergency registration will overwrite any previous emergency registration.

7) the S-CSCF shall not send any third-party REGISTER requests to any AS;

8) determine the duration of the registration by checking the value of the registration expiration interval value in the received REGISTER request and based on local policy; and

NOTE 5: The value of the emergency registration time is subject to national regulation and can be subject to roaming agreements.

9) for any bindings created by the emergency registration, mark those bindings as created by an emergency registration.

### 5.4.8.3 User-initiated emergency deregistration

When S-CSCF receives a REGISTER request with the registration expiration interval value containing zero and the Contact header field contains a contact address that has been registered for emergency service (i.e. the "sos" SIP URI parameter that indicates that this is an emergency registration is included in the Contact header field), the S-CSCF shall reject the REGISTER request by sending a 501 (Not Implemented) response.

NOTE: The UE cannot deregister its emergency public user identity.

### 5.4.8.4 Network-initiated emergency deregistration

The S-CSCF shall not perform a network-initiated emergency deregistration.

### 5.4.8.5 Network-initiated emergency reauthentication

If a given public user identity and the associated contact address have been registered via emergency registration, the S-CSCF shall not reauthenticate this public user identity.

### 5.4.8.6 Subscription to the event providing registration state

If a S-CSCF receives a SUBSCRIBE request addressed to S-CSCF containing the Event header field with the reg event package with the Contact header field that contains a contact address that has been registered for emergency service, the S-CSCF shall reject the SUBSCRIBE request for the reg-event package by sending a 489 (Bad Event) response.

### 5.4.8.7 Notification of the registration state

When the user performs an emergency registration or when the emergency registration expires, the S-CSCF shall not send a NOTIFY request to the subscribers to the reg event package of the respective user.

The contact address that has been registered for emergency services shall not be included in the NOTIFY requests sent to the subscribers to the reg event package of the user.

## 5.5 Procedures at the MGCF

### 5.5.1 General

The MGCF, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem. Therefore table A.4/1 and dependencies on that major capability shall not apply.

The use of the Path and Service-Route header fields shall not be supported by the MGCF.

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;



the MGCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs.

**NOTE:** The special treatment can include filtering, higher priority processing, routing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

When the MGCF sends any request or response related to a dialog, the MGCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses header fields before sending the message.

The MGCF shall use a GRUU referring to itself (as specified in RFC 5627 [93]) when inserting a contact address in a dialog establishing or target refreshing SIP message. This specification does not define how GRUUs are created by the MGCF; they can be provisioned by the operator or obtained by any other mechanism. A GRUU used by the MGCF when establishing a dialog shall remain valid for the lifetime of the dialog. The GRUU used by the MGCF shall not reveal calling party related information.

The MGCF shall handle requests addressed to its currently valid GRUUs when received outside of the dialog in which the GRUU was provided.

**EXAMPLE:** Upon receipt of an INVITE request addressed to a GRUU assigned to a dialog it has active, and containing a Replaces header field referencing that dialog, the MGCF will be able to establish the new call replacing the old one.

The MGCF may support retrieval of NP data, subject to local policy. The interface used at the MGCF to retrieve the NP data is out of scope of this specification. Retrieval of NP data is relevant only if the Request-URI contains an international public telecommunications number. For requests from the IM CN subsystem network, if the Request-URI contains a tel-URI with an "npdi" tel-URI parameter, as defined in RFC 4694 [112], NP data has been obtained previously and NP data retrieval is not needed, but still may still be performed if required by local policy. If NP data is retrieved by the MGCF, and the request is routed to the IM CN subsystem, the MGCF shall add the tel-URI NP parameters to the Request-URI as defined in RFC 4694 [112]: an "npdi" tel-URI parameter is added to indicate that NP data retrieval has been performed, and if the number is ported, an "rn" tel-URI parameter is added to identify the ported-to routing number.

The MGCF NP procedures also apply when the request contains a Request-URI in the form of a SIP URI user=phone, where the "npdi" and "rn" tel-URI parameters are contained in the userinfo part of the SIP URI.

The MGCF supports as a network option the inclusion of the XML MIME schema for PSTN. In cases where the XML MIME for PSTN is included the Content-Type header field is set to "application/vnd.etsi.pstn+xml" and the Content-Disposition to "signal" with the "handling" parameter set to "optional".

## 5.5.2 Subscription and notification

Void.

## 5.5.3 Call initiation

### 5.5.3.1 Initial INVITE

#### 5.5.3.1.1 Calls originated from circuit-switched networks

When the MGCF receives an indication of an incoming call from a circuit-switched network, the MGCF shall:

- 1) generate an INVITE request:
  - set the Request-URI to the "tel" format using an E.164 address or to the "sip" format using an E164 address in the user portion and set user=phone;

**NOTE 1:** Details how to set the host portion are out of scope of the document. However, when a SIP URI is used the host portion needs to be part of the domain name space owned by the I-CSCF

- include the "100rel" option tag in the Supported header field (as defined in RFC 3262 [27]);
- include the "precondition" option tag in the Supported header field (as defined in RFC 3312 [30] as updated by RFC 4032 [64]) if the MGCF supports the SIP preconditions mechanism;

- not indicate the requirement for the precondition mechanism by using the Require header field;
- include an P-Asserted-Identity header field, including the display name if available, depending on corresponding information in the circuit-switched network;

NOTE 2: Inclusion of P-Asserted-Identity header depends on existence of calling party number in Initial Address Message, according to subclause 7.2.3.2.2.3 of 3GPP TS 29.163 [11B] which defines mapping of Bearer Independent Call Control/ISDN User Part Parameter fields to SIP P-Asserted-Identity header fields, and the header field may or may not appear in the request.

- create a new, globally unique value for the "icid-value" header field parameter and insert it into the P-Charging-Vector header field; and
- insert a type 2 "orig-ioi" header field parameter into the P-Charging-Vector header field. The MGCF shall set the type 2 "orig-ioi" header field parameter to a value that identifies the sending network in which the MGCF resides and the type 2 "term-ioi" header field parameter shall not be included.

When the MGCF receives a 1xx or 2xx response to an initial request for a dialog, the MGCF shall store the value of the received "term-ioi" header field parameter received in the P-Charging-Vector header field, if present.

NOTE 3: Any received "term-ioi" header field parameter will be a type 2 IOI. The type 2 IOI identifies the sending network of the response message.

Upon receiving a 199 (Early Dialog Terminated) provisional response to an established early dialog the MGCF shall release resources specifically related to that early dialog.

Based upon local policy, the MGCF may support preferred circuit carrier access (RFC 4694 [112]). If such routing is applicable for the call, the MGCF shall perform the interworking of the carrier identification code from the circuit switched signalling protocol as described in 3GPP TS 29.163 [11B]. The "cic" tel-URI parameter is added in the tel-URI or in the userinfo part of the SIP URI with user=phone Request-URI in accordance with RFC 4694 [112].

If resource priority in accordance with RFC 4412 [116] is required for a dialog, then the MGCF shall include the Resource-Priority header field in all requests associated with that dialog.

If overlap signalling using the multiple-INVITE method is supported as a network option, several INVITE requests with the same Call ID and the same From header field (including "tag" header field parameter) that relate to the same call can be sent by the MGCF. The MGCF shall route those INVITE requests to the same next hop.

#### 5.5.3.1.2 Calls terminating in circuit-switched networks

When the MGCF receives an initial INVITE request with Supported header field indicating "100rel", the MGCF shall:

- 1) store the value of the "orig-ioi" header field parameter received in the P-Charging-Vector header field, if present;

NOTE: Any received "orig-ioi" header field parameter will be a type 2 IOI. The type 2 IOI identifies the sending network of the request message.

- 2) send a 100 (Trying) response;
- 3) after a matching codec is found or no codec is required at the MGW, send 183 "Session Progress" response:
  - set the Require header field to the value of "100rel";
  - store the values received in the P-Charging-Function-Addresses header field;
  - store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field; and
  - insert a P-Charging-Vector header field containing the "orig-ioi" header field parameter, if received in the initial INVITE request and a type 2 "term-ioi" header field parameter. The MGCF shall set the type 2 "term-ioi" header field parameter to a value that identifies the network in which the MGCF resides and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter.

If a codec is required and the MGCF does not find an available matching codec at the MGW for the received initial INVITE request, the MGCF shall:

- send 503 (Service Unavailable) response if the type of codec was acceptable but none were available; or

- send 488 (Not Acceptable Here) response if the type of codec was not supported, and may include SDP in the message body to indicate the codecs supported by the MGCF/MGW.

Based upon local policy, the MGCF may support preferred circuit carrier access (RFC 4694 [112]), if such routing is applicable for the call.

NOTE: Interworking of the "cic" tel-URI parameter, if present in a tel-URI or in the userinfo part of a SIP URI with user=phone Request-URI, to the circuit switched signalling protocol is described in 3GPP TS 29.163 [11B].

The MGCF may support resource priority in accordance with RFC 4412 [116] if required for a dialog. The MGCF shall use compatible namespace and priority levels to the capabilities supported in the CS network.

### 5.5.3.2 Subsequent requests

#### 5.5.3.2.1 Calls originating in circuit-switched networks

When the MGCF receives 183 (Session Progress) response to an INVITE request, the MGCF shall:

- store the values received in the P-Charging-Function-Addresses header field.

The MGCF shall send an UPDATE request when the following conditions are fulfilled:

- conditions as specified in 3GPP TS 29.163 [11B]; and
- the MGCF receives 200 (OK) response to a PRACK request

#### 5.5.3.2.2 Calls terminating in circuit-switched networks

When the MGCF receives an indication of a ringing for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 180 (Ringing) response to the UE.

When the MGCF receives an indication of answer for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 200 (OK) response to the UE. The 200 (OK) response shall include an P-Asserted-Identity header field if corresponding information is received from the circuit-switched network.

## 5.5.4 Call release

### 5.5.4.1 Call release initiated by a circuit-switched network

When the MGCF receives an indication of call release from a circuit-switched network, the MGCF shall:

- send a BYE request to the UE.

### 5.5.4.2 IM CN subsystem initiated call release

NOTE: The release of a call towards the circuit-switched network additionally requires signalling procedures other than SIP in the MGCF that are outside the scope of this document.

### 5.5.4.3 MGW-initiated call release

When the MGCF receives an indication from the MGW that the bearer was lost, the MGCF shall:

- send a BYE request towards the UE; and
- may include Error-Info header field with a pointer to additional information indicating that bearer was lost.

## 5.5.5 Call-related requests

### 5.5.5.1 ReINVITE

#### 5.5.5.1.1 Calls originating from circuit-switched networks

Void.

#### 5.5.5.1.2 Calls terminating in circuit-switched networks

When the MGCF receives a reINVITE request for hold/resume operation, the MGCF shall:

- send 100 (Trying) response;
- after performing interaction with MGW to hold/resume the media flow, send 200 (OK) response.

## 5.5.6 Further initial requests

When the MGCF responds to an OPTIONS request with a 200 (OK) response, the MGCF may include a message body with an indication of the DTMF capabilities and supported codecs of the MGCF/MGW.

NOTE: The detailed interface for requesting MGCF/MGW capabilities is not specified in this version of the document. Other solutions can be used in the interim.

## 5.6 Procedures at the BGCF

### 5.6.1 General

The use of the Path and Service-Route header fields shall not be supported by the BGCF.

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the BGCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs.

NOTE: The special treatment can include filtering, higher priority processing, routing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

When the BGCF receives any request or response (excluding ACK requests and CANCEL requests and responses) related to a dialog or standalone transaction, the BGCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses header fields before forwarding the message.

With the exception of 305 (Use Proxy) responses, the BGCF may recurse on a 3xx response only when the domain part of the URI contained in the 3xx response is in the same domain as the BGCF. For the same cases, if the URI is an IP address, the BGCF shall only recurse if the IP address is known locally to be an address that represents the same domain as the BGCF.

### 5.6.2 Common BGCF procedures

When determining where to route the received request, the originating BGCF may use the information obtained from other protocols or any other available databases.

The BGCF may support retrieval of NP data as part of the procedures to determine where to route the request. Retrieval of NP data by the BGCF is subject to local policy. Retrieval of NP data is relevant only if the Request-URI contains an international public telecommunications number. The interface used at the BGCF to retrieve the NP data is out of scope of this specification. If the Request-URI contains a tel-URI with an "npdi" tel-URI parameter, as defined in RFC 4694 [112], NP data has been obtained previously and NP data retrieval is only performed if required by local policy. If NP data is retrieved by the BGCF, the BGCF shall add the tel-URI NP parameters to the Request-URI as defined in RFC 4694 [112]: an "npdi" tel-URI parameter is added to indicate that NP data retrieval has been performed,

and if the number is ported, an "rn" tel-URI parameter is added to identify the ported-to routing number. The "rn" tel-URI parameter may be used by the BGCF for routing the request.

The BGCF NP procedures also apply when the request contains a Request-URI in the form of a SIP URI user=phone, where the "npdi" and "rn" tel-URI parameters are contained in the userinfo part of the SIP URI.

When the BGCF receives a request, the BGCF shall forward the request:

- to an MGCF within its own network; or
- to another network containing a BGCF, or I-CSCF; or
- where the request is for another network, to an IBCF in its own network, if local policy requires IBCF capabilities towards another network; or
- where the Ici interface is used to interconnect two networks and the destination network is beyond such interface, to an IBCF in its own network..

When forwarding the request to the next hop, the BGCF may leave the received Request-URI unmodified.

If the request is not routed to a BGCF or to an entity that implements the additional routing functionality, the BGCF shall remove the P-Served-User header field prior to forwarding the request.

When the BGCF receives a request and the Request-URI contains a tel URI in local number format or a SIP URI with the user part not starting with a + and the "user" SIP URI parameter equals "phone", the BGCF shall not forward the request to an entity in another network (e.g. BGCF, I-CSCF) unless the local policy (e.g. routing of service numbers) requires forwarding the request outside the network. If local policy does not allow forwarding the request outside the network and additional routing capabilities as defined in Annex I are locally available, the BGCF shall attempt translation of the local number. If the translation fails, the BGCF shall send an appropriate SIP response to the originator. If local policy does not allow forwarding the request outside the network and additional routing capabilities as defined in annex I are not locally available, the BGCF shall either:

- forward the request to any appropriate entity in its own network where additional routing functionality are available; or
- send an appropriate SIP response to the originator.

The BGCF need not Record-Route the INVITE and the SUBSCRIBE requests. While the next entity may be a MGCF acting as a UA, the BGCF shall not apply the procedures of RFC 3323 [33] relating to privacy. The BGCF shall store the values received in the P-Charging-Function-Addresses header field. The BGCF shall store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field and retain the "icid-value" header field parameter in the P-Charging-Vector header field.

NOTE 1: The means by which the decision is made to forward to an MGCF or to another network is outside the scope of the present document, but can be by means of a lookup to an external database, or can be by data held internally to the BGCF.

If the BGCF supports carrier routing, then the BGCF shall support the following procedures, based on local policy:

- a) if the BGCF is configured to populate an operator configured preassigned carrier into a tel-URI contained in the Request-URI, and a preassigned carrier is required for this call, then the BGCF shall include the "cic" tel-URI parameter in the Request-URI identifying the preassigned carrier (as described in RFC 4694 [112]); or
- b) if the BGCF is configured to populate the freephone carrier ID, and a freephone carrier is required for this call, then the BGCF shall include the "cic" tel-URI parameter in the Request-URI identifying the freephone carrier (as described in RFC 4694 [112]).

The BGCF carrier routing procedures also apply when the Request-URI is in the form of a SIP URI user=phone, where the "cic" tel-URI parameter is contained in the userinfo part of the SIP URI.

The BGCF shall not add the "cic" tel-URI parameter in the Request-URI if the parameter already exists in the tel-URI.

NOTE 2: Local policy should be able to control the interaction and precedence between routing on "cic" parameter versus routing based on "rn" parameter.

NOTE 3: The means to configure the BGCF with the pre-assigned carrier is outside the scope of this document.

### 5.6.3 Specific procedures for INVITE requests and responses

When the BGCF receives an INVITE request that contains a Feature-Caps header field with the "+g.3gpp.home-visited" header field parameter, the BGCF shall decide based on local policy whether to perform loopback routing for this request. The BGCF shall:

- a) if loopback routing is not to be performed for this request remove any "+g.3gpp.trf" or "+g.3gpp.home-visited" header field parameter from the Feature-Caps header field of the outgoing request;
- b) if loopback routing is applied for this request:
  - i) remove all entries in the Route header field;
  - ii) if a "+g.3gpp.trf" header field parameter with a parameter value containing a valid URI, is included in the Feature-Caps header field of the request, insert the URI in a Route header field;
  - iii) if a "+g.3gpp.trf" header field parameter, with a parameter value containing a valid URI is not included in the Feature-Caps header field of the request, insert a locally configured TRF address, associated with the visited network for this call (as identified in the "+g.3gpp.home-visited" header field parameter), in the Route header field;
  - iv) remove any "+g.3gpp.home-visited" header field parameter from the Feature-Caps header field of the outgoing request;
  - v) if included in the incoming request, remove the "+g.3gpp.trf" header field parameter from the Feature-Caps header field from the outgoing request;
  - vi) insert the "+g.3gpp.loopback" header field parameter, as specified in subclause 7.9A.4 in the Feature-Caps header field of the request, in accordance with RFC 6809 [190]. If providing the identifier of the home network is supported by the BGCF and the visited network, the BGCF may based on operator agreement insert the "+g.3gpp.loopback" header field parameter set to the identifier of the home network; and
  - vii) remove the "orig-ioi" header field parameter received in the P-Charging-Vector header field, if present. The BGCF shall insert a type 1 "orig-ioi" header field parameter into the P-Charging-Vector header field and shall set the type 1 "orig-ioi" header field parameter to a value that identifies the home network of the served user (i.e. the network in which the BGCF resides). The BGCF shall not include the "term-ioi" header field parameter; and
- c) if the final decision on loopback routing is deferred to a subsequent entity in the home network, a further BGCF, then, retain in the request a Feature-Caps header field with the "+g.3gpp.home-visited" header field parameter with the parameter value set to the identifier of the visited network. The BGCF is expected to know by means of network configuration that such a subsequent entity exists;

If the BGCF inserts its own Record-Route header field, the BGCF may require the periodic refreshment of the session to avoid hung states in the BGCF. If the BGCF requires the session to be refreshed, the BGCF shall apply the procedures described in RFC 4028 [58] clause 8.

**NOTE:** Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

If overlap signalling using the multiple-INVITE method is supported as a network option, several INVITE requests with the same Call ID and the same From header field (including "tag" header field parameter) can be received outside of an existing dialog. Such INVITE requests relate to the same call and the BGCF shall route such INVITE request received during a certain period of time to the same next hop.

If the BGCF inserted in the initial request for the dialog the header field parameters into the Feature-Caps header field then the BGCF shall include the header field parameters with the same parameter values into the Feature-Caps header field in any target refresh request for the dialog, and in each 1xx or 2xx response to target refresh request sent in the same direction.

## 5.7 Procedures at the Application Server (AS)

### 5.7.1 Common Application Server (AS) procedures

#### 5.7.1.1 Notification about registration status

The AS may support the REGISTER method in order to discover the registration status of the user. If a REGISTER request arrives and the AS supports the REGISTER method, the AS shall store the registration expiration interval value from the request and generate a 200 (OK) response or an appropriate failure response. For the success case, the 200 (OK) response shall contain a registration expiration interval value equal to the value received in the REGISTER request. The AS shall store the values received in P-Charging-Function-Addresses header field. Also, the AS shall store the values of the "icid-value" header field parameter and "orig-ioi" header field parameter if present in the P-Charging-Vector header field from the REGISTER request. The AS shall insert a P-Charging-Vector header field containing the "orig-ioi" header field parameter, if received in the REGISTER request and a type 3 "term-ioi" header field parameter in the response to REGISTER. The AS shall set the type 3 "term-ioi" header field parameter to a value that identifies the service provider from which the response is sent and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter.

Upon receipt of a third-party REGISTER request, with the Content-Type header field or with a MIME body part's Content-Type header field set according to subclause 7.6 (i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field or a MIME body part's Content-Type header field, independent of the value or presence of Content-Disposition parameters or MIME body part's Content-Disposition parameters, then the following treatment is applied:

- if the third-party REGISTER request includes an IM CN subsystem XML body with an <ims-3gpp> element, including a version attribute, with the <service-info> child element or a MIME body part containing an <ims-3gpp> element with a <service-info> XML child element as described in subclause 7.6, then the AS may retrieve the service information within the <service-info> XML child element of the <ims-3gpp> element.

Upon receipt of a third-party REGISTER request, with the Content-Type header field or with a body part's Content-Type header field set to "message/sip" and including a "message/sip" MIME body of the incoming REGISTER request, or the 200 (OK) response to the incoming REGISTER request then the AS may retrieve information from the "message/sip" MIME body or body part.

Upon receipt of a third-party REGISTER request, the AS may subscribe to the reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680 [43].

On sending a SUBSCRIBE request, the AS shall populate the header fields as follows:

- a) a Request-URI set to the resource to which the AS wants to be subscribed to, i.e. to a SIP URI that contains the public user identity of the user that was received in the To header field of the third-party REGISTER request;
- b) a From header field set to the AS's SIP URI;
- c) a To header field, set to a SIP URI that contains the public user identity of the user that was received in the To header field of the third-party REGISTER request;
- d) an Event header field set to the "reg" event package;
- e) a P-Asserted-Identity header field set to the SIP URI of the AS; and

NOTE 1: The S-CSCF expects the SIP URI used in the P-Asserted-Identity header field to correspond to the SIP URI, which identified this AS in the initial filter criteria of the user to whose registration state the AS subscribes to.

- f) a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17] and a type 3 "orig-ioi" header field parameter. The type 3 "orig-ioi" header field parameter identifies the service provider from which the request is sent. The AS shall not include the type 3 "term-ioi" header field parameter.

Upon receipt of a 2xx response to the SUBSCRIBE request, the AS shall store the information for the so established dialog and the expiration time as indicated in the Expires header field of the received response.

Upon receipt of any response, the AS shall store the value of the "term-voi" header field parameter received in the P-Charging-Vector header field if present.

NOTE 2: Any received term-voi parameter will be a type 3 term-voi. The type 3 term-voi identifies the network operator from which the response was sent.

NOTE 3: Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header field set to "terminated", the AS considers the subscription to the reg event package terminated, i.e. as if the AS had sent a SUBSCRIBE request with an Expires header field containing a value of zero.

Upon receipt of a NOTIFY request, the AS shall store the value of the "orig-voi" header field parameters if present in the P-Charging-Vector header field. The AS shall insert a P-Charging-Vector header field in the response to the NOTIFY request containing the "orig-voi" header field parameter, if received in the NOTIFY request and a type 3 "term-voi" header field. The AS shall set the type 3 "term-voi" header field parameter to a value that identifies the service provider from which the response is sent and the "orig-voi" header field parameter is set to the previously received value of "orig-voi" header field parameter.

### 5.7.1.2 Extracting charging correlation information

When an AS receives an initial request for a dialog or a request (excluding ACK requests and CANCEL requests and responses) for a standalone transaction, the AS shall store the values received in the P-Charging-Vector header field, e.g. "orig-voi" header field parameter, if present, and "icid-value" header field parameter, and retain the P-Charging-Vector header field in the message. The AS shall store the values received in the P-Charging-Function-Addresses header field and retain the P-Charging-Function-Addresses header field in the message.

When an AS sends any request or response related to a dialog or standalone transaction, the AS may insert previously saved values into the P-Charging-Vector and P-Charging-Function-Addresses header fields before sending the message.

### 5.7.1.3 Access-Network-Info and Visited-Network-ID

The AS may receive in any request or response (excluding ACK requests and CANCEL requests and responses) information about the served user access network. The AS may receive information about the served user core network in REGISTER requests from S-CSCF. This information can be obtained either from the P-Access-Network-Info header field and P-Visited-Network-ID header field in the REGISTER request or can be obtained from those header fields in the body of the REGISTER request. The AS can use the header fields to provide an appropriate service to the user.

### 5.7.1.3A Determination of the served user

#### 5.7.1.3A.1 General

The determination of the served user is different per session:

- for an originating session, the procedure is described in subclause 5.7.1.3A.2; and
- for a terminating session the procedure is described in subclause 5.7.1.3A.3.

If the AS supports the P-Served-User header field as defined in RFC 5502 [133] and the P-Served-User header field is included in the received request, the AS can determine the session case related to the request, as specified in 3GPP TS 29.228 [14], from the P-Served-User header field parameters if available.

#### 5.7.1.3A.2 AS serving an originating user

If an AS receives a request on behalf of an originating user:

- and the AS supports the P-Served-User header field as defined in RFC 5502 [133], the AS shall determine the served user by taking the identity contained in the P-Served-User header field if available;
- otherwise, if the AS supports the History-Info header field as defined in RFC 4244 [66] the AS shall determine the served user from the content of the History-Info header field if available; and
- otherwise, the AS shall determine the served user by taking the identity contained in P-Asserted-Identity header field.



### 5.7.1.3A.3 AS serving a terminating user

If an AS receives a request on behalf of a terminating user:

- and the AS supports the P-Served-User header field as defined in RFC 5502 [133], the AS shall determine the served user by taking the identity contained in the P-Served-User header field if available;
- otherwise, if the AS supports the History-Info header field as defined in RFC 4244 [66] the AS shall determine the served user from the content of the History-Info header field if available, or from the content of the Request-URI; and
- otherwise, the AS shall determine the served user from the content of the Request-URI.

### 5.7.1.4 User identify verification at the AS

The procedures at the AS to accomplish user identity verification are described with the help of figure 5-1.

NOTE: Different means can be used to represent or transport the credentials. Such mechanisms are subject to operator policy and can e.g. include the P-Asserted-Identity header field, the Authorization header field or other mechanisms not specified by 3GPP TS 24.229.

When the AS receives a SIP initial or standalone request, excluding REGISTER request, that does not contain credentials, the AS shall:

- a) if a Privacy header field is present in the initial or standalone request and the Privacy header field value is set to "id" or "user", then the user and the request are considered as anonymous, and no further actions are required. The AS shall consider the request as authenticated;
- b) if there is no Privacy header field present in the initial or standalone request, or if the Privacy header field contains a value other than "id" or "user", then the AS shall check for the presence of a P-Asserted-Identity header field in the initial or standalone request. Two cases exist:
  - i) the initial or standalone request contains a P-Asserted-Identity header field. This is typically the case when the user is located inside a trusted domain as defined by subclause 4.4. In this case, the AS is aware of the identity of the user and no extra actions are needed. The AS shall consider the request as authenticated.
  - ii) the initial or standalone request does not contain a P-Asserted-Identity header field. This is typically the case when the user is located outside a trusted domain as defined by subclause 4.4. In this case, the AS does not have a verified identity of the user. The AS shall check the From header field of the initial or standalone request. If the From header field value in the initial or standalone request is set to "Anonymous" as specified in RFC 3261 [26], then the user and the request are considered as anonymous and no further actions are required. If the From header field value does not indicate anonymity, then the AS shall challenge the user by issuing a 401 (Unauthorized) response including a challenge as per procedures described in RFC 3261 [26].

When the AS receives a SIP initial or standalone request that contains credentials but it does not contain a P-Asserted-Identity header field the AS shall check the correctness of the credentials as follows:

- a) If the credentials are correct, then the AS shall consider the identity of the user verified, and the AS shall consider the request as authenticated;
- b) If the credentials are not correct, the AS may either rechallenge the user by issuing a 401 (Unauthorized) response including a challenge as per procedures described in RFC 3261 [26] (up to a predetermined maximum number of times predefined in the AS configuration data), or consider the user as anonymous. If the user is considered anonymous, the AS shall consider the request as authenticated.

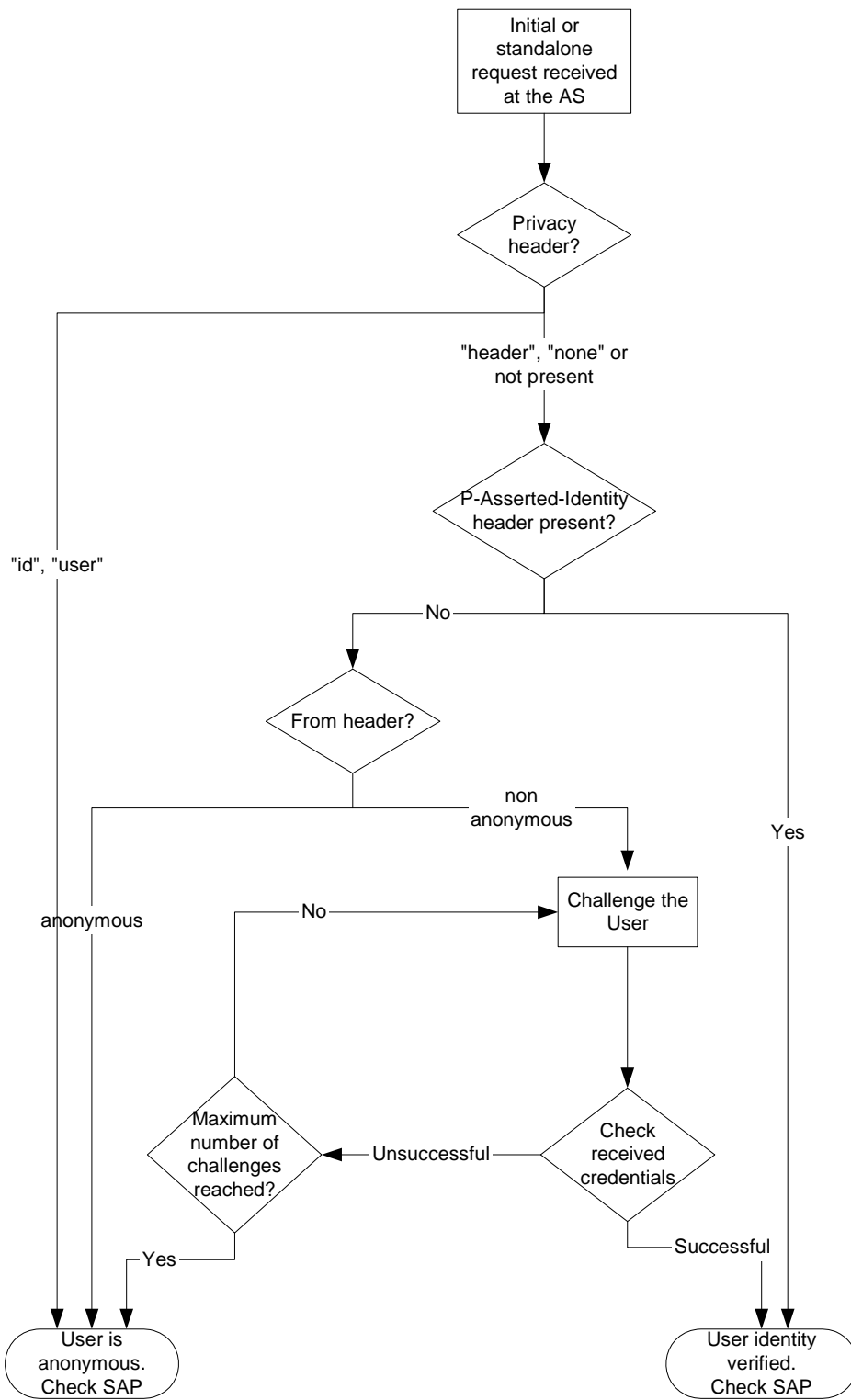


Figure 5-1: User identity verification flow at the AS

### 5.7.1.5 Request authorization

Once the AS have tried to verify the identity of the user, the AS either has a verified identity of the user or it considers the user as anonymous.

If the user is considered anonymous, the AS shall check whether the authorization policy defined for this request allows anonymous requests. If anonymous requests are allowed, then the AS can proceed with the requested functionality, otherwise, the AS shall not proceed with the requested functionality.

If the user is identified by an identity, the AS shall apply the authorization policy related to the requested functionality to detect whether the particular user is allowed to request the functionality. The authorization policy may require a verified identity of a user.

If the request is authorized then the AS shall continue with the procedures as defined for that request.

If the request is not authorized, the AS shall either:

- reject the request according to the procedures defined for that request e.g., by issuing a 403 (Forbidden) response; or
- send a 2xx final response if the authorization policy requires to deny the requested functionality, whilst appearing to the user as if the request has been granted.

### 5.7.1.6 Event notification throttling

If the AS has a local configuration information limiting the rate at which notification generation is allowed, then the AS shall take that information into account. Such local configuration information could be e.g. the shortest time period between issuing consecutive NOTIFY requests.

### 5.7.1.7 Local numbering

#### 5.7.1.7.1 Interpretation of the numbers in a non-international format

If home operator's local policy defines a prefix string(s) to enable subscribers to differentiate dialling a geo-local number and/or a home-local number and if the phone number in a non-international format in the Request-URI includes such a prefix, the AS shall interpret the received number in a non-international format as a geo-local number or as a home-local number according to the prefix.

If the phone number in a non-international format in the Request-URI includes a "phone-context" tel URI parameter, the AS shall:

- 1) if the "phone-context" tel URI parameter contains access technology information or the home domain name prefixed by the "geo-local." string, interpret it as a geo-local number;
- 2) if the "phone-context" tel URI parameter contains the home domain name, interpret it as a home-local number; or
- 3) if the "phone-context" tel URI parameter contains any other value, apply general procedures for translation.

NOTE 1: If business communication services are provided to the calling user, and the "phone-context" tel URI parameter contains a value associated with a private numbers, it is expected that any needed translation of the number information is handled by the corresponding business communication AS.

If the phone number in a non-international format in the Request-URI includes both operator defined prefix and a "phone-context" tel URI parameter and those information are contradictory, the AS shall ignore either the prefix or the "phone-context" tel URI parameter according to operator policy.

If the phone number in a non-international format in the Request-URI does not include either a "phone-context" tel URI parameter or an operator defined prefix, the AS shall interpret the phone number in a non-international format either as a geo-local number or as a home-local number according to operator policy.

NOTE 2: Operator must ensure that service setting dialling strings do not reach local numbering AS by setting appropriately the precedences of the initial filter criteria.

### 5.7.1.7.2 Translation of the numbers in a non-international format

When an AS receives a request having a geo-local number in a non-international format in the Request-URI, the AS shall use the "phone-context" tel URI parameter to determine the visited access network, if the "phone-context" tel URI parameter in the Request-URI is available. If the "phone-context" tel URI parameter in the Request-URI is not available, the AS may determine the visited access network based on the available P-Access-Network-Info header fields containing the access-type field, if it is available in the received request, or by means outside the scope of this document.

If the visited access network is determined:

- 1) if the home network supports the roaming architecture for voice over IMS with local breakout, and an incoming INVITE request contains a Feature-Caps header field with the "+g.3gpp.home-visited" header field parameter, the AS may choose to not attempt translation of some geo-local numbers and defer the translation to the visited network after loopback has been performed; or
- 2) the AS shall attempt to determine whether the geo-local number:
  - a) corresponds to a home local service number that can be used by a roaming user;
  - b) is used to access a service in the visited network; or
  - c) is used to access the local addressing plan of the visited network;

and translate the received geo-local number to a globally routeable SIP URI or an international tel URI:

NOTE 1: During the translation the AS can contact an entity in the visited access network for getting the needed information. The protocol and procedures for this is outside the scope of this specification.

NOTE 2: The AS can translate the tel URI to a SIP URI by including the 'telephone-subscriber' part of the received tel URI to the user part of the SIP URI and setting the domain name of the SIP URI to indicate the domain name of the network of the phone number based on the received "phone-context" tel URI parameter.

NOTE 3: In addition to the service numbers corresponding to a service in the visited network the home network can also support service numbers corresponding to services in the home network as geo-local service numbers.

When an AS receives a request having a home-local number in a non-international format in the Request-URI, the AS shall determine whether the home-local number is used to access a service or the local addressing plan and translate the received home-local number to a globally routeable SIP URI or an international tel URI:

When an AS receives a request having any other number in a non-international format in the Request-URI, the AS shall attempt to determine whether it is used to access a service in the third network or the local addressing plan of the third network and translate the received number in a non-international format to a globally routeable SIP URI or an international tel URI:

NOTE 4: The AS can translate the tel URI to a SIP URI by including the 'telephone-subscriber' part of the received tel URI to the user part of the SIP URI and setting the domain name of the SIP URI to indicate the domain name of the network of the phone number based on the received "phone-context" tel URI parameter;

NOTE 5: If business communication services are provided to the calling user, and the "phone-context" tel URI parameter contains a value associated with a private numbers, it is expected that any needed translation of the number information is handled by the corresponding business communication AS.

If the translation at the AS fails, the AS shall either send an appropriate SIP response or leave the Request-URI unmodified and route the request based on the topmost Route header field, based on local policy.

### 5.7.1.8 GRUU assignment and usage

It is possible for an AS to use a GRUU referring to itself when inserting a contact address in a dialog establishing or target refreshing SIP message.

This specification does not define how GRUUs are created by the AS; they can be provisioned by the operator or obtained by any other mechanism. The GRUU shall remain valid for the time period in which features addressed to it remain meaningful.

The AS shall handle requests addressed to its currently valid GRUUs when received outside of the dialog in which the GRUU was provided.

**EXAMPLE:** Upon receipt of an INVITE request addressed to a GRUU assigned to a dialog it has active, and containing a Replaces header field referencing that dialog, the AS will be able to establish the new call replacing the old one, if that is appropriate for the features being provided by the AS.

When an AS is acting as a routing B2BUA (as defined in subclause 5.7.5) it may provide a contact address that is not a GRUU when the contact address in the incoming message that is being replaced is not a GRUU.

When an AS is acting as a routing B2BUA forwards a SIP request it shall transparently forward a received Contact header field when the Contact header field contains a GRUU. When transparently forwarding a received Contact header field of a dialog-forming request, the AS shall include its own URI in a Record-Route header field in order to ensure that it is included on the route of subsequent requests.

When an AS acts as UA or Initiating B2BUA it may provide a contact address that is not a GRUU in cases where it can ascertain that valid requests that could result from the use of that contact and follow the usage rules of RFC 5627 [93] will reach the element. In all other cases the AS shall use a GRUU.

An AS acting as a UA or an initiating B2BUA on behalf of a public user identity can provide a GRUU in the contact address referring to itself as described above. When the AS provides a GRUU on behalf of a user, subsequent dialog-initiating requests sent to that GRUU will be routed directly to the AS, thus bypassing terminating services assigned to the user. If the AS wishes to have terminating services applied for the user, the AS may generate a new terminating request addressed to a public GRUU associated with the public user identity of the user.

**NOTE 1:** If the AS wishes to have terminating services applied when the public user identity on whose behalf the AS is acting is unregistered, then the options available to the AS depend on whether or not the subscriber has ever previously registered with the IM CN subsystem. In the case where the public user identity had previously registered with the IM CN subsystem, then the AS can use the most recently allocated public GRUU if available. In the case where the user has never registered with the IM CN subsystem, then the AS can use the public user identity itself.

**NOTE 2:** Once terminating services have been applied, it is assumed that the terminating S-CSCF will route the request back to this AS via the initial filter criteria. In order for this to work, the initial filter criteria of the target user need to be configured so that the AS is invoked at the appropriate time relative to other terminating ASs (say, after the required terminating services have been applied). The mechanism to ensure that the AS is invoked by the initial filter criteria at the appropriate time is outside the scope of this specification (e.g. the user's filter criteria could be statically configured to invoke the AS at the correct time, or the AS could use the Dynamic Service Activation Information mechanism to activate the appropriate filter criteria).

When an AS acts as a UA or an initiating B2BUA, and is originating or terminating a request on behalf of a public user identity, and privacy is required, the AS shall ensure that any GRUU provided in the contact address in the request does not reveal the public user identity of the user.

### 5.7.1.9 Use of ICSI and IARI values

Based on service logic, an AS can validate an ICSI value received in an Accept-Contact header field or received in a P-Asserted-Service header field and reject the request if necessary.

A trusted AS may insert a P-Asserted-Service header field in a request for a new dialog or standalone transaction. An untrusted AS may insert a P-Preferred-Service header field in a request for a new dialog or standalone transaction. If the request is related to an IMS communication service that requires the use of an ICSI then the AS:

- shall include the ICSI value (coded as specified in subclause 7.2A.8.2), for the IMS communication service that is related to the request in either a P-Asserted-Service header field or a P-Preferred-Service header field depending whether the AS is trusted or not according to RFC 6050 [121].

When an AS that is acting as a UA or initiating B2BUA or routing B2BUA sends an initial request for a dialog or a request for a standalone transaction, the AS may include an Accept-Contact header field containing:

- an ICSI value (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3841 [56B]; and
- one or more IARI values (coded as specified in subclause 7.2A.9.2) that are related to the request in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3841 [56B];

if the ICSI or IARIs for the IMS communication service and IMS application are known.

The AS may:

- include the received ICSI and IARI values;
- replace or remove received ICSI and IARI values; or
- include new ICSI and IARI values.

When the AS acting as a UA or initiating B2BUA or routing B2BUA sends a SIP request or a SIP response related to an IMS communication service, the AS may include in the Contact header field:

- in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 one or more ICSI values (coded as specified in subclause 7.2A.8.2); and
- one or more IARI values (coded as specified in subclause 7.2A.9.2) in a g.3gpp.iari-ref media feature tag, for the IMS applications, that are related to the request as defined in subclause 7.9.2 and RFC 3840 [62];

if the ICSI or IARIs for the IMS communication service and IMS application are known. The AS may:

- include the received ICSI and IARI values;
- replace or remove received ICSI values; or
- include new ICSI and IARI values.

When sending a 18x or 2xx response to a request on behalf of an originating user, then the AS may insert a Feature-Caps header field with the "+g.3gpp.icsi-ref" header field parameter into the response, as specified in RFC 6809 [190]. The parameter value is set according to subclause 7.9A.2.

NOTE 3: The AS can insert the Feature-Caps header field e.g. based on operator policy, IMS communication service specification or depending whether other AS already inserted the Feature-Caps header field with the "+g.3gpp.icsi-ref" header field parameter in the response.

When sending a request on behalf of a terminating user, then the AS may insert a Feature-Caps header field with the "+g.3gpp.icsi-ref" header field parameter. The parameter value is set according to subclause 7.9A.2.

NOTE 4: The AS can insert the Feature-Caps header field e.g. based on operator policy, IMS communication service specification or depending whether other AS already inserted the Feature-Caps header field with the "+g.3gpp.icsi-ref" header field parameter in the request.

If the AS inserted the header field parameters in the Feature-Caps header field in the request or in 18x or 2xx response to request then the AS shall include the header field parameters with the same parameter values into the Feature-Caps header field in any target refresh request, and in each 1xx or 2xx response to target refresh request sent in the same direction.

### 5.7.1.10 Carrier selection

An AS may play a role in support of carrier selection as defined in RFC 4694 [112].

NOTE 1: In general, ASs do not need to support carrier selection, Rather a specific AS or a few ASs in a network will be used for carrier selection,

When an AS that supports carrier selection receives an initial request with a Request-URI in the form of a tel-URI that contains a "cic" tel-URI parameter inserted by the UE and if configured per operator policy, the AS may validate the value of the "cic" parameter. If an AS that supports carrier selection determines the "cic" parameter received in the initial request to be valid, as configured per operator policy, the AS shall process the request accordingly. If an AS supports carrier selection and determines the "cic" parameter received in the initial request to be invalid, then the AS shall remove the "cic" parameter and process the request as if no "cic" had been received from the UE.

When an AS that support carrier selection receives an initial request with a Request-URI in the form of a tel-URI, the AS may, based on operator policy, insert an appropriate value for the "cic" tel-URI parameter as defined in RFC 4694 [112].

NOTE 2: For example, the AS that supports preferred carrier could insert a "cic" tel-URI parameter that identifies the originating user's preassigned carrier, or the carrier assigned to a called freephone number.

When an AS that support carrier selection receives an initial request with a Request-URI in the form of a SIP URI user=dialstring (see RFC 4967 [103]), the AS may translate the SIP URI to a valid tel-URI or a valid SIP URI user=phone comprising a userinfo part containing the tel-URI and a domain matching the domain of the original SIP URI user=dialstring. If the received SIP URI user=dialstring is successfully converted, then the AS shall replace the Request-URI with the newly created tel-URI or SIP URI user=phone. The AS shall then process the request as if it had arrived from the UE containing this tel-URI or SIP URI user=phone in the Request-URI.

NOTE 3: This specification does not make any assumptions regarding how these procedures are mapped to ASs; whether all procedures are supported by a single AS or spread across multiple ASs. However, this specification does assume that the responsibility for ensuring that the UE complies with the carrier selection procedures defined in RFC 4694 [112] will be performed by a single AS (e.g. validate "cic"), and the filter criteria will be configured so that this AS is invoked before other ASs that have carrier selection responsibilities.

The AS carrier selection procedures also apply when the request contains a Request-URI in the form of a SIP URI user=phone, where the "cic" tel-URI parameter is contained in the userinfo part of the SIP URI.

#### 5.7.1.11 Void

#### 5.7.1.12 Delivery of original destination identity

If the service the AS provides needs to deliver the original destination identity to the UE, the AS shall insert a new hi-entry to the last hi-entry of History-Info header field including "mp" header field parameter as specified in subclause 7.2A.16.

NOTE: If the "mp" header field parameter is present in the hi-entries within the History-Info header field, the information of the original destination number or URI, e.g. the service number for freephone, will be found in the hi-entry whose index-val matches the value of the first hi-entry with "mp" header field parameter.

#### 5.7.1.13 CPC and OLI

The AS may populate the "cpc" and "oli" URI parameters in each initial request for a dialog or a request for a standalone transaction in the tel URI or SIP URI representation of telephone numbers in the P-Asserted-Identity header field based on their origin source.

#### 5.7.1.14 Emergency transactions

Identification of emergency transactions for termination in the public network by an AS are outside the scope of this document, and are dependent on many application specific considerations.

Where an AS decides to generate an emergency request on behalf of its served user, the AS shall meet the following conditions:

- 1) the UE is in the same network as the S-CSCF (i.e. that the UE is not roaming).

NOTE 1: How the above is determined is outside the scope of this document and will depend on the application supported. Possible mechanisms could be: 1) that the AS only receives requests that are from non-roaming UEs; 2) analysis of the P-Access-Network-Info header field in a received request from the UE.

The AS generate the request with the following contents:

- 1) include in the Request-URI an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]. An additional sub-service type can be added if information on the type of emergency service is known;
- 2) a Route header field with the topmost Route header field set to the URI associated with an E-CSCF;

- 3) if the AS is part of the trust domain of the network, a P-Asserted-Identity header field containing the identity of the UE served by the AS;
- 4) if the AS is not part of the trust domain of the network, a P-Preferred-Identity header field containing the identity of the UE served by the AS;
- 5) if a GRUU is available for the UE served by the AS, provide the GRUU as part of a Contact header field;

NOTE 2: If the AS is not already aware of the GRUU of the UE due to previously receiving it in a Contact header, and the UE is registered, the GRUU can be obtained using either the subscription to the reg events package or using the 3rd party registration procedure with the REGISTER request including a "message/sip" MIME body of the 200 (OK) response for the REGISTER request as described in subclause 5.7.1.1.

- 6) if a location is available at the AS in any form, include a Geolocation header field with that location; and
- 7) a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17].

If the AS does not receive any response to the INVITE request (including its retransmissions); or receives a 3xx response or 480 (Temporarily Unavailable) response to an INVITE request, the AS shall select a new E-CSCF and forward the INVITE request.

### 5.7.1.15 Protecting against attacks using 3xx responses

The AS upon receiving a 3xx response to a request from the served UE that contains a Contact header field may remove the Contact header field or modify the response code from 3xx to an appropriate non 2xx response code (e.g. 5xx response code) based on operator policy before sending the response towards the UE.

NOTE: Automatically recursing on untrusted 3xx responses opens up the UE to being redirected to premium rate URIs without the user's consent. An AS that protects against attacks using 3xx responses needs to ensure that it doesn't break services that depend on 3xx responses being passed to the UE. Subclause 5.1.2A.1.1 specifies how a UE protects itself against attacks using 3xx responses. For some services an AS could automatically recurse on a 3xx response.

### 5.7.1.16 Support of Roaming Architecture for Voice over IMS with Local Breakout

#### 5.7.1.16.1 Preservation of parameters

An AS in a network supporting the roaming architecture for voice over IMS with local breakout shall not change the value of the "icid" header field parameter in the P-Charging-Vector header field received in the INVITE request when the AS sends any request or response related to an INVITE transaction.

NOTE: An AS that determines that loopback is not a viable option can change or remove any of the above parameters if required by the application logic performed by the AS.

#### 5.7.1.16.2 Preference for loopback routing not to occur

When the AS is accessed by a network supporting roaming architecture for voice over IMS with local breakout, and the incoming INVITE request contains a Feature-Caps header field with the "+g.3gpp.home-visited" header field parameter, the AS can indicate to the S-CSCF its preference for loopback routing not to occur by removing the "+g.3gpp.home-visited" header field parameter from the Feature-Caps header field from any outgoing INVITE request back to the S-CSCF. Reasons for such an indication might include the need to terminate media streams at an MRF in the home network.

NOTE: If the original dialog identifier sent by the S-CSCF is not preserved by the AS in the outgoing requests, then loopback routing will not occur.

### 5.7.1.17 Delivery of network provided location information

If the AS supports delivery of network provided location information, and the AS performs the retrieval of cell id and/or UE time zone via Sh interface, the AS shall insert the P-Access-Network-Info header field with the cell id and/or local-time-zone parameter, including a "network-provided" parameter in the incoming request or response. The P-Access-Network-Info header shall only be inserted if there is not already a network provided information.



### 5.7.1.18 Delivery of MRB address information

A visited MRB address can be received during session establishment. If an AS receives the URI of an MRB in a "+g.3gpp.mrb" header field parameter included in a Feature-Caps header field of an INVITE request, it shall store this URI. If the AS requests allocation of MRF resources from an MRB in its own network, either in in-line or query mode, the AS shall forward the visited network MRB URI in the request.

### 5.7.1.19 Overload control

#### 5.7.1.19.1 Outgoing subscriptions to load-control event

Based on operator policy, the AS may subscribe to the load-control event package with one or more target SIP entities. The list of target SIP entities is provisioned.

Subscription to the load-control event package is triggered by internal events (e.g. the physical device hosting the SIP entity is power-cycled) or through a management interface.

The AS shall perform subscriptions to the load-control event package to a target entity in accordance with RFC 3265 [28] and with RFC 7200 [201]. When subscribing to the load-control event, the AS shall:

- 1) Send a SUBSCRIBE request in accordance with RFC 3265 [28] and with RFC 7200 [201] to the target entity, with the following elements:
  - an Expires header field set to a network specific value;
- 2) If the target entity is located in a different network and local policy requires the application of IBCF capabilities, forward the request to an IBCF acting as an exit point.

The AS shall automatically refresh ongoing subscriptions to the load-control event package either 600 seconds before the expiration time if the initial subscription was for greater than 1200 seconds, or when half of the time has expired if the initial subscription was for 1200 seconds or less.

The AS can terminate a subscription according to RFC 3265 [28].

#### 5.7.1.19.2 Incoming subscriptions to load-control event

If subscriptions to load-control event package is supported, the AS shall handle incoming subscriptions to the load-control event package in accordance with RFC 3265 [28] and with RFC 7200 [201]. When the AS receives a SUBSCRIBE request for the load-control event from an unauthorised or unexpected source, the AS shall generate a "403 forbidden" response to the SUBSCRIBE request.

If the AS receives a SUBSCRIBE request from an authorised source the AS shall:

- 2) Generate a "200 OK" response to the SUBSCRIBE request with the following settings:
  - an Expires header field, set to either the same or a decreased value as the Expires header field in SUBSCRIBE request; and
  - the Contact header field set to an identifier uniquely associated to the SUBSCRIBE request that may help correlating refreshes.
- 3) In case of an initial subscription, determine the list of load filters applicable to the subscriber, create an XML document to represent this information and send it as an attachment to a NOTIFY request towards the subscriber. If no applicable load filters are identified when the subscription request is received, an empty document is attached to the NOTIFY request.

Subsequent NOTIFY requests with updated or new filters may then be sent as the actual load of the target entity evolves.

### 5.7.2 Application Server (AS) acting as terminating UA, or redirect server

When acting as a terminating UA the AS shall behave as defined for a UE in subclause 5.1.4, with the exceptions identified in this subclause.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

If the AS requires knowledge of the served user it shall determine the served user according to the applicable procedure in subclause 5.7.1.3A.

An AS acting as redirect server shall propagate any received IM CN subsystem XML message body in the redirected message.

When an AS acting as a terminating UA generates a subsequent request that does not relate to an INVITE dialog, the AS shall insert a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17].

When the AS acting as terminating UA receives an initial request for a dialog or a request for a standalone transaction, the AS shall store the value of the "orig-ioi" header field parameters received in the P-Charging-Vector header field if present.

NOTE: Any received orig-ioi parameter will be a type 3 orig-ioi. The orig-ioi identifies the network operator from which the request was sent.

When the AS acting as terminating UA generates a response to an initial request for a dialog or a request for a standalone transaction, the AS shall insert a P-Charging-Vector header field containing the "orig-ioi" header field parameter, if received in the request and a type 3 "term-ioi" header field parameter. The AS shall set the type 3 "term-ioi" header field parameter to a value that identifies the service provider from which the response is sent and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter.

If resource priority in accordance with RFC 4412 [116] is required for a dialog, then the AS shall include the Resource-Priority header field in all requests associated with that dialog.

### 5.7.3 Application Server (AS) acting as originating UA

In order to support an AS acting as an originating UA, the AS has to be within the same trust domain as the S-CSCF to which requests will be sent.

When acting as an originating UA the AS shall behave as defined for a UE in subclause 5.1.3, with the exceptions identified in this subclause.

The AS, although acting as a UA, does not initiate any registration of its associated addresses and does not participate in any authentication procedures defined for a UE. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

When an AS acting as an originating UA generates an initial request for a dialog or a request for a standalone transaction, the AS shall insert a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17] and a type 3 "orig-ioi" header field parameter. The AS shall set the type 3 "orig-ioi" header field parameter to a value that identifies the service provider from which the request is sent. The AS shall not include the type 3 "term-ioi" header field parameter.

NOTE 1: The AS can retrieve CDF and/or ODF addresses from HSS on Sh interface.

When the AS acting as an originating UA receives any response to an initial request for a dialog or a request for a standalone transaction, the AS shall store the value of the "term-ioi" header field parameter received in the P-Charging-Vector header field if present.

NOTE 2: Any received "term-ioi" header field parameter will be a type 3 IOI. The type 3 IOI identifies the network operator from which the response was sent.

When an AS acting as an originating UA generates a subsequent request that does not relate to an INVITE dialog, the AS shall insert a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17].

The AS shall extract charging function addresses from any P-Charging-Function-Addresses header field that is received in any 1xx or 2xx responses to the requests.

The AS may also indicate that the proxies should not fork the request by including a "no-fork" directive within the Request-Disposition header field in the request as described in RFC 3841 [56B].

When sending any initial request, an identity is needed that will correlate with the service profile to be used at the S-CSCF. If the identity for that service profile corresponds to the value to be used to identify the caller to the destination user, include the identity in the P-Asserted-Identity header field. If the identity for that service profile does not correspond to the value to be used to identify the caller to the destination user, and the P-Served-User header field is supported by the S-CSCF, include the identity in the P-Served-User header field. This leaves the P-Asserted-Identity header field for the identity to be used to identify the caller to the destination user. If the identity for that service profile matches a wildcarded identity and the P-Profile-Key header field is supported by the AS, include the wildcarded identity in the P-Profile-Key header field.

When sending an initial request on behalf of a PSI that is hosted by the AS, the AS shall:

- insert a Request-URI as determined by the service logic;
- insert a P-Asserted-Identity header field and possibly a P-Served-User header field containing the PSI as indicated earlier in this subclause;
- if the AS is not able to resolve the next hop address by itself or the operator policy does not allow it, insert a Route header field pointing either to the S-CSCF where the PSI is hosted, or to the entry point of the home network of the PSI or to the transit function. The AS shall append the "orig" parameter to the URI in the topmost Route header field; and

NOTE 3: The address of the S-CSCF hosting the PSI can be obtained by querying the HSS on the Sh interface.

NOTE 4: AS can only send the initial request to the entry point of the home network of the PSI only if the AS can assume (e.g. based on local configuration) that the receiving entry point will be able to process the request as an originating request.

- if the AS is able to resolve the next hop address by itself and the operator policy allows it, forward the originating request directly to the destination without involving any S-CSCF in the originating IM CN subsystem.

When sending an initial request on behalf of a public user identity, the AS shall:

- insert a Request-URI as determined by the service logic;
- insert a P-Asserted-Identity header field and possibly a P-Served-User header field containing the public user identity as indicated earlier in this subclause;
- if the AS intends to send the originating request to the home network of the public user identity or the operator policy requires it, insert a Route header field pointing to the S-CSCF where the public user identity on whose behalf the request is generated is registered or hosted (unregistered case) or to the entry point of the public user identity's network. The AS shall append the "orig" parameter to the URI in the topmost Route header field; and

NOTE 5: The address of the S-CSCF can be obtained either by querying the HSS on the Sh interface or during third-party registration.

NOTE 6: AS can send the initial request to the entry point of the public user identity's network or to the entry point of the home network of the PSI only if the AS can assume (e.g. based on local configuration) that the receiving entry point will be able to process the request as an originating request.

- if the AS intends to send the originating request directly to the terminating network and the operator policy allows it, forward the originating request directly to the destination without involving any S-CSCF in the originating IM CN subsystem.

When sending an initial request to a served public user identity, the AS shall insert:

- a Request-URI containing the served public user identity;
- a P-Asserted-Identity as determined by the service logic (e.g. the URI of the AS or the URI of the entity that triggered the SIP request, if the sending of the initial request is triggered by a non-SIP request); and
- a Route header field pointing to the S-CSCF where the public user identity to whom the request is generated is registered or hosted (unregistered case) or to the entry point of the public user identity's network. The AS shall not append the "orig" parameter to the URI in the topmost Route header field.

NOTE 7: The address of the S-CSCF can be obtained either by querying the HSS on the Sh interface or during third-party registration.

The AS can indicate privacy of the P-Asserted-Identity in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the AS shall set the From header field to "Anonymous" as specified in RFC 3261 [26].

NOTE 8: The contents of the From header field cannot be relied upon to be modified by the network based on any privacy specified by the user either within the AS indication of privacy or by network subscription or network policy. Therefore the AS includes the value "Anonymous" whenever privacy is explicitly required.

If resource priority in accordance with RFC 4412 [116] is required for a dialog, then the AS shall include the Resource-Priority header field in all requests associated with that dialog.

## 5.7.4 Application Server (AS) acting as a SIP proxy

When the AS acting as a SIP proxy receives a request from the S-CSCF, prior to forwarding the request, the AS shall:

- remove its own URI from the topmost Route header field; and
- after executing the required services, route the request based on the topmost Route header field.

The AS may modify the SIP requests based on service logic, prior to forwarding the request back to the S-CSCF.

The AS shall not fork the request if the fork-directive in the Request-Disposition header field is set to "no-fork" as described in RFC 3841 [56B].

If the AS requires knowledge of the served user it shall determine the served user according to the applicable procedure in subclause 5.7.1.3A.

An AS acting as a SIP proxy shall propagate any received IM CN subsystem XML message body in the forwarded message.

When the AS acting as a SIP proxy receives an initial request for a dialog or a request for a standalone transaction, the AS shall store the value of the "orig-ioi" header field parameter received in the P-Charging-Vector header field if present. The AS shall remove the "orig-ioi" header field parameter from the forwarded request and insert a type 3 "orig-ioi" header field parameter. The AS shall set the type 3 "orig-ioi" header field parameter to a value that identifies the service provider from which the request is sent. The AS shall not include the type 3 "term-ioi" header field parameter.

NOTE: A received orig-ioi parameter will be a type 3 orig-ioi. The orig-ioi identifies the network operator from which the request was sent.

When the AS acting as a SIP proxy forwards a response to an initial request for a dialog or a request for a standalone transaction, the AS shall remove any received "orig-ioi" and "term-ioi" header field parameters, and insert a P-Charging-Vector header field containing the previously stored "orig-ioi" header field parameter, if received in the request and a type 3 "term-ioi" header field parameter. The AS shall set the type 3 "term-ioi" header field parameter to a value that identifies the service provider from which the response is sent and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter. Any values of "orig-ioi" or "term-ioi" header field parameters received in any response that is being forwarded are not used.

## 5.7.5 Application Server (AS) performing 3rd party call control

### 5.7.5.1 General

The AS performing 3rd party call control acts as a B2BUA. There are two kinds of 3rd party call control:

- Routing B2BUA: an AS receives a request, terminates it and generates a new request, which is based on the received request.
- Initiating B2BUA: an AS initiates two requests, which are logically connected together at the AS, or an AS receives a request and initiates a new request that is logically connected but unrelated to the incoming request

from the originating user (e.g. the P-Asserted-Identity of the incoming request is changed by the AS). AS can initiate additional requests and associate them with a related incoming request.

When the AS acting as an initiating B2BUA receives a request and initiates a new request that is logically connected but unrelated to the incoming request from the originating user, the AS can include an original dialog identifier in the Route header field for the S-CSCF that it learned from the incoming request, per service logic needs.

NOTE 1: If the AS does not include the original dialog identifier in an initiated request, the S-CSCF can apply the default handling procedure relating to the incoming request if after a certain time no 1xx response is sent by the AS to the incoming request or if the AS forwards a 408 (Request Timeout) response or a 5xx response received from downstream as a response to the the incoming request. To avoid the application of the default handling procedure by the S-CSCF when the AS is waiting for a SIP response for an initiated request, the AS can generate a SIP provisional response to the incoming request.

If the AS requires knowledge of the served user the AS shall determine the served user according to the applicable procedure in subclause 5.7.1.3A.

When the AS receives a terminated call and generates a new call, and dependent on whether the service allows the AS to change the P-Asserted-Identity for outgoing requests compared with the incoming request, the AS will select appropriate kind of 3rd party call control.

The B2BUA AS will internally map the message header fields between the two dialogs that it manages. It is responsible for correlating the dialog identifiers and will decide when to simply translate a message from one dialog to the other, or when to perform other functions. These decisions are specific to each AS and are outside the scope of the present document.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

For standalone transactions, when the AS is acting as a Routeing B2BUA, the AS shall copy the remaining Route header field(s) unchanged from the received request for a standalone transaction to the new request for a standalone transaction.

When the AS receives a Replaces header field within an initial request for a dialog, the AS should check, whether the AS acts as a routeing B2BUA for the dialog identified in the Replaces header field. The AS should:

- if the AS acts as routeing B2BUA for the dialog indicated in the Replaces header field, include in the forwarded request a Replaces header field, indicating the the dialog on the outgoing side that corresponds to the dialog identified in the received Replaces header field; or
- if the AS does not act as a routeing B2BUA for the dialog indicated in the Replaces header field, include in the forwarded request the Replaces header field as received in the incoming request.

When the AS acting as a routeing B2BUA receives an initial request for a dialog or a request for a standalone transaction, the AS shall:

- store the value of the "orig-ioi" header field parameter received in the P-Charging-Vector header field if present; and
- remove the "orig-ioi" header field parameter from the forwarded request.

NOTE 2: Any received orig-ioi parameter will be a type 3 orig-ioi. The orig-ioi identifies the network operator from which the request was sent.

When an AS acts as a routeing B2BUA and the received Contact header field contains a media feature tag indicating a capability for which the Contact URI can be used by the remote party, the AS shall transparently forward the Contact header field. When transparently forwarding a received Contact header field of a dialog-forming request, the AS shall include its own URI in a Record-Route header field in order to ensure that it is included on the route of subsequent requests.

NOTE 3: One example of such a media feature tag is the isfocus media feature tag where the URI in the Contact header field is used by conference services to transport the temporary conference identity that can be used when rejoining an ongoing conference.

When the AS acting as a routing B2BUA generates a response to an initial request for a dialog or a request for a standalone transaction, the AS shall insert a P-Charging-Vector header field containing the "orig-ioi" header field parameter, if received in the request and a type 3 "term-ioi" header field parameter. The AS shall set the type 3 "term-ioi" header field parameter to a value that identifies the service provider from which the response is sent and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter. Any values of "orig-ioi" or "term-ioi" header field parameter received in any response that is being forwarded are not used.

The AS shall transparently pass supported and unsupported signalling elements (e.g. SIP headers, SIP messages bodies), except signalling elements that are modified or deleted as part of the hosted service logic, or based on service provider policy.

If resource priority in accordance with RFC 4412 [116] is required for a dialog, then the AS shall include the Resource-Priority header field in all requests associated with that dialog.

## 5.7.5.2 Call initiation

### 5.7.5.2.1 Initial INVITE

When the AS acting as a Routing B2BUA receives an initial INVITE request, the AS shall:

- 1) remove its own SIP URI from the topmost Route header field of the received INVITE request;
- 2) perform the AS specific functions. See 3GPP TS 23.218 [5];
- 3) if successful, generate and send a new INVITE request to establish a new dialog;
- 4) copy the remaining Route header field(s) unchanged from the received INVITE request to the new INVITE request;
- 5) copy the P-Asserted-Identity to the outgoing request;
- 6) if a Route header field is present, route the new INVITE request based on the topmost Route header field; and

NOTE 1: The topmost Route header field of the received INVITE request will contain the AS's SIP URI. The following Route header field will contain the SIP URI of the S-CSCF.

- 7) if no Route header field is present (e.g. the AS may be acting on behalf of a PSI):
  - a) insert a Route header field pointing either to the S-CSCF where the PSI is hosted or to the entry point of the home network of the PSI or to the transit function, if the AS is not able to resolve the next hop address by itself or the operator policy requires it; or
  - b) forward the originating request directly to the destination without involving any S-CSCF in the originating IM CN subsystem, if the AS is able to resolve the next hop address by itself, and the operator policy allows it.

NOTE 2: The address of the S-CSCF hosting the PSI can be obtained by querying the HSS on the Sh interface.

When the AS is acting as an Initiating B2BUA, the AS shall apply the procedures described in subclause 5.7.3 for any outgoing requests. The AS shall either set the "icid-value" header field parameter in the P-Charging-Vector header field to be the same as received or different.

NOTE 3: The AS can retrieve CDF and/or ODF addresses from HSS on Sh interface.

### 5.7.5.2.2 Subsequent requests

Void.

## 5.7.5.3 Call release

## 5.7.5.4 Call-related requests

An AS may initiate a call release. See 3GPP TS 23.218 [5] for possible reasons. The AS shall simultaneously send the BYE request for both dialogs managed by the B2BUA.

### 5.7.5.5 Further initial requests

When the AS is acting as an Initiating B2BUA the AS shall apply the procedures described in subclause 5.7.3 for the requests. The AS shall either set the "icid-value" header field parameter in the P-Charging-Vector header field to be the same as received or different. The AS may initiate any number of requests, per service logic needs.

### 5.7.5.6 Transcoding services invocation using third-party call control

An AS may invoke transcoding at an MRFC by the use of RFC 4117 [166], if the MRFC supports acting as the transcoding server described in RFC 4117 [166].

During the call setup, an AS may decide proactively to invoke transcoding when receiving an INVITE request, or reactively when the callee rejects the call setup using a 488 (Not Acceptable Here) response. To invoke transcoding using RFC 4117 [166], the AS shall act as a B2BUA between caller and callee and establish a third SIP dialogue towards the MRFC offering the codecs supported by the caller and the codecs to be offered towards the callee, and the IP address and port information received from caller, in separate media lines. When receiving an answer from the MRFC, the AS shall forward the received selected codecs and IP address and port information in the callee's media line(s) as an offer towards the callee. When the callee answers with selected codecs and IP address and port information, the AS shall forward this information within a new offer to the MRFC. When receiving the corresponding answer from the MRFC, the AS shall forward the address and port information within the caller's media line(s) as an answer towards the caller.

The SIP messages relating to the dialogue between AS and MRFC are sent either via the S-CSCF over the ISC and Mr interfaces, or directly over the Mr' interface.

## 5.7.6 Void

## 5.8 Procedures at the MRFC

### 5.8.1 General

Although the MRFC is acting as a UA, it is outside the scope of this specification how the MRFC associated addresses are made known to other entities.

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the MRFC shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs.

**NOTE:** This special treatment can include filtering, higher priority processing, routing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

When the MRFC sends any request or response (excluding ACK requests and CANCEL requests and responses) related to a dialog or standalone transaction, the MRFC may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses header fields before sending the message.

The MRFC shall use a GRUU referring to itself (as specified in RFC 5627 [93]) when inserting a contact address in a dialog establishing or target refreshing SIP message. This specification does not define how GRUUs are created by the MRFC; they can be provisioned by the operator or obtained by any other mechanism. A GRUU used by the MRFC when establishing a dialog shall remain valid for the lifetime of the dialog.

The MRFC shall handle requests addressed to its currently valid GRUUs when received outside of the dialog in which the GRUU was provided.

**EXAMPLE:** Upon receipt of an INVITE request addressed to a GRUU assigned to a dialog it has active, and containing a Replaces header field referencing that dialog, the MRFC will be able to establish the new call replacing the old one.

## 5.8.2 Call initiation

### 5.8.2.1 Initial INVITE

#### 5.8.2.1.1 MRFC-terminating case

##### 5.8.2.1.1.1 Introduction

The MRFC shall provide a P-Asserted-Identity header field in a response to the initial request for a dialog, or any response for a standalone transaction. It is a matter of network policy whether the MRFC expresses privacy according to RFC 3323 [33] with such responses.

When the MRFC receives an initial INVITE request, the MRFC shall store the values received in the P-Charging-Vector header field, e.g. "icid-value" header field parameter. The MRFC shall store the values received in the P-Charging-Function-Addresses header field.

##### 5.8.2.1.1.2 Tones and announcements

The MRFC can receive INVITE requests to set up a session to play tones and announcements. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request for a tone or announcement, the MRFC shall:

- send 100 (Trying) response.

##### 5.8.2.1.1.3 Ad-hoc conferences

The MRFC can receive INVITE requests to set up an ad-hoc conferencing session (for example a multiparty call) or to add parties to the conference. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request for ad hoc conferencing, the MRFC shall:

- send 100 (Trying) response.

When the MRFC receives an INVITE request to add a party to an existing ad hoc conference (i.e. MRFC conference identifier), the MRFC shall:

- send 100 (Trying) response.

##### 5.8.2.1.1.4 Transcoding

The MRFC may receive INVITE requests to set up transcoding between endpoints with incompatible codecs. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request for transcoding and a codec is supplied in SDP, the MRFC shall:

- send 100 (Trying) response.

When the MRFC receives an INVITE request with an indicator for transcoding but no SDP, the MRFC shall:

- send 183 (Session Progress) response with list of codecs supported by the MRFC/MRFP.

#### 5.8.2.1.2 MRFC-originating case

The MRFC shall provide a P-Asserted-Identity header field in an initial request for a dialog, or any request for a standalone transaction. It is a matter of network policy whether the MRFC expresses privacy according to RFC 3323 [33] with such requests.

When an MRFC generates an initial request for a dialog or a request for a standalone transaction, the MRFC shall insert a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17].



## 5.8.2.2 Subsequent requests

### 5.8.2.2.1 Tones and announcements

When the MRFC receives an ACK request for a session, this may be considered as an event to direct the MRFP to start the playing of a tone or announcement.

### 5.8.2.2.2 Transcoding

When the MRFC receives a PRACK request (in response to the 183 (Session Progress) response with an indicator for transcoding and codec supplied in SDP, the MRFC shall:

- after the MRFP indicates that the transcoding request is granted, send 200 (OK) response.

## 5.8.3 Call release

### 5.8.3.1 S-CSCF-initiated call release

#### 5.8.3.1.1 Tones and announcements

When the MRFC receives a BYE request for a session, the MRFC directs the MRFP to stop the playing of a tone or announcement.

### 5.8.3.2 MRFC-initiated call release

#### 5.8.3.2.1 Tones and announcements

When the MRFC has a timed session to play tones and announcements and the time expires, the MRFC shall:

- send a BYE request towards the UE.

When the MRFC is informed by the MRFP that tone or announcement resource has been released, the MRFC shall:

- send a BYE request towards the UE.

## 5.8.4 Call-related requests

### 5.8.4.1 ReINVITE

#### 5.8.4.1.1 MRFC-terminating case

##### 5.8.4.1.1.1 Ad-hoc conferences

The MRFC can receive reINVITE requests to modify an ad-hoc conferencing session (for example a multiparty call) for purposes of floor control and for parties to leave and rejoin the conference.

When the MRFC receives a reINVITE request, the MRFC shall:

- send 100 (Trying) response; and
- after the MRFP indicates that the conferencing request is granted, send 200 (OK) response. The MRFC may choose to send a 183 (Session Progress) response prior to the 200 (OK) response.

#### 5.8.4.1.2 MRFC-originating case

Void.

### 5.8.4.2 REFER

#### 5.8.4.2.1 MRFC-terminating case

Void.

#### 5.8.4.2.2 MRFC-originating case

Void.

#### 5.8.4.2.3 REFER initiating a new session

Void.

#### 5.8.4.2.4 REFER replacing an existing session

Void.

#### 5.8.4.3 INFO

Void.

### 5.8.5 Further initial requests

When the MRFC responds to an OPTIONS request with a 200 (OK) response, the MRFC may include a message body with an indication of the supported tones/announcement packages, DTMF capabilities, supported codecs and conferencing options of the MRFC/MRFP.

**NOTE:** As specified in RFC 6230 [146] an MRFC supporting the use of the control channel framework shall support the SYNC command to indicate the media control packages supported. Additionally each media control package should define an audit command for discovery of package capabilities (for example supported codecs and options).

## 5.8A Procedures at the MRB

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the MRB shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs.

**NOTE:** This special treatment can include filtering, higher priority processing, routing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

## 5.9 Void

### 5.9.1 Void

## 5.10 Procedures at the IBCF

### 5.10.1 General

As specified in 3GPP TS 23.228 [7] border control functions may be applied between two IM CN subsystems or between an IM CN subsystem and other SIP-based multimedia networks based on operator preference. The IBCF may act both as an entry point and as an exit point for a network. If it processes a SIP request received from other network it functions as an entry point (see subclause 5.10.3) and it acts as an exit point whenever it processes a SIP request sent to other network (see subclause 5.10.2).

The functionalities of the IBCF are entry and exit point procedures as defined in subclause 5.10.2 and subclause 5.10.3 and additionally can include:

- network configuration hiding (as defined in subclause 5.10.4);
- application level gateway (as defined in subclause 5.10.5);
- transport plane control, i.e. QoS control (as defined in subclause 5.10.5);
- screening of SIP signalling (as defined in subclause 5.10.6);
- inclusion of an IWF if appropriate;

- media transcoding control (as defined in subclause 5.10.7); and
- privacy protection (as defined in subclause 5.10.8).

NOTE 1: The functionalities performed by the IBCF are configured by the operator, and it is network specific.

When an IBCF acting as an exit or an entry point receives a SIP request, the IBCF may reject the SIP request based on local policy by sending an appropriate SIP 4xx response.

NOTE 2: The local policy can take bilateral agreements between operators into consideration.

NOTE 3: Some SIP requests can be rejected by an AS instead of the IBCF according to local policy.

The IBCF, acting as B2BUA, which is located between visited network and home network shall preserve the dialog identifier, i.e. shall not change the Call-Id header field value, the "tag" header field parameter value of the From header field in any SIP INVITE request and any SIP response to the SIP INVITE request, and shall preserve the "tag" header field parameter value of the To header field, in any SIP response to the SIP INVITE request.

NOTE 4: The IBCF can identify whether it is located between visited network and home network based on local configuration.

## 5.10.2 IBCF as an exit point

### 5.10.2.1 Registration

When IBCF receives a REGISTER request, the IBCF shall:

- 1) void;
- 2) if network topology hiding is required or IBCF is configured to perform application level gateway and/or transport plane control functionalities, then the IBCF shall add its own routeable SIP URI to the top of the Path header field; and

NOTE 1: The IBCF can include in the inserted SIP URI an indicator that identifies the direction of subsequent requests received by the IBCF i.e., from the S-CSCF towards the P-CSCF, to identify the UE-terminating case. The IBCF can encode this indicator in different ways, such as, e.g., a unique parameter in the URI, a character string in the username part of the URI, or a dedicated port number in the URI.

NOTE 2: Any subsequent request that includes the direction indicator (in the Route header field) or arrives at the dedicated port number, indicates that the request was sent by the S-CSCF towards the P-CSCF.

- 3) select an entry point of the home network and forward the request to that entry point.

If the selected entry point:

- does not respond to the REGISTER request and its retransmissions by the IBCF; or
- sends back a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request;

the IBCF shall select a new entry point and forward the REGISTER request to that entry point.

NOTE 3: The list of the entry points can be either obtained as specified in RFC 3263 [27A] or provisioned in the IBCF. The entry point can be an IBCF or an I-CSCF.

If the IBCF fails to forward the REGISTER request to any entry point, the IBCF shall send back a 504 (Server Time-Out) response to the P-CSCF, in accordance with the procedures in RFC 3261 [26].

#### 5.10.2.1A General

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field or a temporarily authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the IBCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs.

NOTE: The special treatment can include filtering, higher priority processing, routing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

Based on local policy, the IBCF acting as an exit point shall add in responses in the P-Charging-Vector header field a "transit-voi" header field parameter with an entry which identifies the operator network which the response is transiting or with a void entry.

Based on local policy the IBCF shall delete or void in responses in the P-Charging-Vector header field any received "transit-voi" header field parameter value.

### 5.10.2.2 Initial requests

Upon receipt of:

- an initial request for a dialog;
- a request for a standalone transaction, except the REGISTER method; or
- a request for an unknown method that does not relate to an existing dialog;

the IBCF shall:

- 1) if the request is an INVITE request, respond with a 100 (Trying) provisional response;
- 2) if the request is an INVITE request and the IBCF is configured to perform application level gateway and/or transport plane control functionalities, save the Contact, CSeq and Record-Route header field values received in the request such that the IBCF is able to release the session if needed;
- 2A) If the request is a SUBSCRIBE and the IBCF does not need to act as B2BUA, based on operator policy, the IBCF shall determine whether or not to retain, for the related subscription, the SIP dialog state information and the duration information;

NOTE 1: The event package name can be taken into account to decide whether or not the SIP dialog state and the subscription duration information needs to be retained.

NOTE 2: The IBCF needs to insert its own URI in Record-Route of SUBSCRIBE if it decides to retain the SIP dialog state information.

- 2B) if the request is an initial request for a dialog and local policy requires the application of IBCF capabilities in subsequent requests, perform record route procedures as specified in RFC 3261 [26];
- 3) void;
- 4) void;
- 5) void;
- 5A) if the recipient of the request is understood from configured information to always send and receive private network traffic from this source, remove the P-Private-Network-Indication header field containing the domain name associated with that saved information;
- 6) store the values from the P-Charging-Function-Addresses header field, if present;
- 7) remove some of the parameters from the P-Charging-Vector header field or the header field itself, depending on operator policy, if present; and
- 8) remove the P-Charging-Function-Addresses header fields, if present, prior to forwarding the message;

and forwards the request according to RFC 3261 [26].

NOTE 3: If IBCF processes a request without a pre-defined route (e.g. the subscription to reg event package originated by the P-CSCF), the next-hop address can be either obtained as specified in RFC 3263 [27A] or be provisioned in the IBCF.

When the IBCF receives an INVITE request, the IBCF may require the periodic refreshment of the session to avoid hung states in the IBCF. If the IBCF requires the session to be refreshed, the IBCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 4: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

With the exception of 305 (Use Proxy) responses, the IBCF shall not recurse on 3xx responses.

### 5.10.2.3 Subsequent requests

Upon receipt of a subsequent request, the IBCF shall:

- 1) if the request is an INVITE request, respond with a 100 (Trying) provisional response;
- 1A) if the request is a NOTIFY request with the Subscription-State header field set to "terminated" and the IBCF has retained the SIP dialog state information for the associated subscription, once the NOTIFY transaction is terminated, the IBCF can remove all the stored information related to the associated subscription;
- 2) if the request is a target refresh request and the IBCF is configured to perform application level gateway and/or transport plane control functionalities, save the Contact and CSeq header field values received in the request such that the IBCF is able to release the session if needed; and
- 3) if the subsequent request is other than a target refresh request (including requests relating to an existing dialog where the method is unknown) and the IBCF is configured to perform application level gateway and/or transport plane control functionalities, save the Contact and CSeq header field values received in the request such that the IBCF is able to release the session if needed;

and forwards the request, based on the topmost Route header field, in accordance with the procedures of RFC 3261 [26].

### 5.10.2.4 IBCF-initiated call release

If the IBCF provides transport plane control functionality and receives an indication of a transport plane related error the IBCF may:

- 1) generate a BYE request for the terminating side based on information saved for the related dialog; and
- 2) generate a BYE request for the originating side based on the information saved for the related dialog.

NOTE: Transport plane related errors can be indicated from e.g. TrGW, or PCRF. The protocol for indicating transport plane related errors to the IBCF is out of scope of this specification.

Upon receipt of the 2xx responses for both BYE requests, the IBCF shall release all information related to the dialog and the related multimedia session.

## 5.10.3 IBCF as an entry point

### 5.10.3.1 Registration

When IBCF receives a REGISTER request, the IBCF shall:

- 1) verify if it arrived from a trusted domain or not. If the request arrived from an untrusted domain, respond with 403 (Forbidden) response;

NOTE 1: The IBCF can find out whether the request arrived from a trusted domain or not, from the procedures described in 3GPP TS 33.210 [19A].

- 2) if network topology hiding, or screening of SIP signalling, is required or IBCF is configured to perform application level gateway and/or transport plane control functionalities, add its own routeable SIP URI to the top of the Path header field; and

NOTE 2: The IBCF can include in the inserted SIP URI an indicator that identifies the direction of subsequent requests received by the IBCF i.e., from the S-CSCF towards the P-CSCF, to identify the UE-terminating case. The IBCF can encode this indicator in different ways, such as, e.g., a unique parameter in the URI, a character string in the username part of the URI, or a dedicated port number in the URI.

NOTE 3: Any subsequent request that includes the direction indicator (in the Route header field) or arrives at the dedicated port number, indicates that the request was sent by the S-CSCF towards the P-CSCF.

3) If IBCF is colocated with an I-CSCF, or it has a preconfigured I-CSCF to be contacted, forward the request to that I-CSCF. Otherwise select an I-CSCF and forward the request to that I-CSCF.

NOTE 4: The selection of an I-CSCF can lead to additional delays.

If the selected I-CSCF:

- does not respond to the REGISTER request and its retransmissions by the IBCF; or
- sends back a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request;

the IBCF shall select a new I-CSCF and forward the REGISTER request to that I-CSCF.

NOTE 5: The list of the I-CSCFs can be either obtained as specified in RFC 3263 [27A] or provisioned in the IBCF.

If the IBCF fails to forward the REGISTER request to any I-CSCF, the IBCF shall send back a 504 (Server Time-Out) response towards the P-CSCF, in accordance with the procedures in RFC 3261 [26].

### 5.10.3.1A General

For all SIP transactions identified:

- if priority is supported (NOTE 1), as containing an authorised Resource-Priority header field or a temporarily authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field;

the IBCF shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs.

NOTE 1: For an INVITE request, various mechanisms can be applied to recognize the need for priority treatment (e.g., based on the dialled digits). The exact mechanisms are left to national regulation and network configuration.

Based on the alternative mechanism to recognize the need for priority treatment, the IBCF shall insert the temporarily authorised Resource-Priority header field with appropriate namespace and priority value in the INVITE request.

NOTE 2: The special treatment can include filtering, higher priority processing, routeing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

Based on local policy, the IBCF acting as an entry point shall add in requests in the P-Charging-Vector header field a "transit-ioi" header field parameter with an entry which identifies the operator network which the request is transitting or with a void entry.

Based on local policy the IBCF shall delete or void in requests in the P-Charging-Vector header field any received "transit-ioi" header field parameter value.

NOTE 3: Only one "transit-ioi" header field parameter entry is added per transit network.

### 5.10.3.2 Initial requests

Upon receipt of:

- an initial request for a dialog;
- a request for a standalone transaction except the REGISTER request; or

- a request for an unknown method that does not relate to an existing dialog;

the IBCF shall verify whether the request is arrived from a trusted domain or not. If the request arrived from an untrusted domain, then the IBCF shall:

- if the topmost Route header field of the request contains the "orig" parameter, respond with 403 (Forbidden) response.

Otherwise,

- remove all P-Charging-Vector header fields and all P-Charging-Function-Addresses header fields the request may contain; and
- remove all Feature-Caps header fields, if present.

Upon receipt of:

- an initial request for a dialog;
- a request for a standalone transaction except the REGISTER request; or
- a request for an unknown method that does not relate to an existing dialog;

the IBCF shall:

- 1) if the request is an INVITE request, then respond with a 100 (Trying) provisional response;
  - 1A) if a P-Private-Network-Indication header field is included in the request, check whether the configured information allows the receipt of private network traffic from this source. If private network traffic is allowed, the IBCF shall check whether the received domain name in any included P-Private-Network-Indication header field in the request is the same as the domain name associated with that configured information. If private network traffic is not allowed, or the received domain name does not match, then the IBCF shall remove the P-Private-Network-Indication header field;
  - 1B) if the initiator of the request is understood from configured information to always send and receive private network traffic from this source, insert a P-Private-Network-Indication header field containing the domain name associated with that configured information;
- 2) if the request is an INVITE request and the IBCF is configured to perform application level gateway and/or transport plane control functionalities, then the IBCF shall save the Contact, CSeq and Record-Route header field values received in the request such that the IBCF is able to release the session if needed;
- 2A) If the request is a SUBSCRIBE and the IBCF does not need to act as B2BUA, based on operator policy, the IBCF shall determine whether or not to retain, for the related subscription, the SIP dialog state information and the duration information;

NOTE 1: The event package name can be taken into account to decide whether or not the SIP dialog state and the subscription duration information needs to be retained.

NOTE 2: The IBCF needs to insert its own URI in Record-Route of SUBSCRIBE if it decides to retain the SIP dialog state information.

- 2B) if the request is an initial request for a dialog and local policy requires the application of IBCF capabilities in subsequent requests, perform record route procedures as specified in RFC 3261 [26];
- 2C) if the request is an initial request for a dialog, or a standalone request, and the Request-URI contains an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69] and a P-Private-Network-Indication valid within the trust domain is not included, include a topmost Route header field set to the URI associated with an E-CSCF. If the network uses the Resource-Priority header field to control the priority of emergency calls, the IBCF shall add a Resource-Priority header field containing a namespace of "esnet" as defined in RFC 7135 [197];
- 3) void;
- 4) If IBCF receives an initial request for a dialog or standalone transaction, that contains a single Route header field pointing to itself, and it is co-located with an I-CSCF, or it has a preconfigured I-CSCF to be contacted, then

forward the request to that I-CSCF. Otherwise select an I-CSCF and forward the request to that I-CSCF. If the single Route header field of the request contains the "orig" parameter, the IBCF shall insert the "orig" parameter to the URI of the I-CSCF; and

NOTE 3: The selection of an I-CSCF can lead to additional delays.

- 5) if the request does not contain a Route header field or if it contains one or more Route header fields where the topmost Route header field does not contain the "orig" parameter, optionally – based on operator policy – append the "orig" parameter to the URI in the topmost Route header field of the next request sent from the IBCF to an entity of the IM CN subsystem for which it is an entry point.

NOTE 4: The appending of an "orig" parameter to the URI in the topmost Route header field enables an IM CN subsystem to perform originating services to the network that originated the initial request. The appending can be dependent on the network that originated the initial request as determined by e.g. origin IP address of the received request, etc.

When the IBCF receives an INVITE request, the IBCF may require the periodic refreshment of the session to avoid hung states in the IBCF. If the IBCF requires the session to be refreshed, the IBCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 5: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

When the IBCF receives a response to an initial request (e.g. 183 or 2xx), the IBCF shall:

- 1) store the values from the P-Charging-Function-Addresses header field, if present; and
- 2) remove the P-Charging-Function-Addresses header field prior to forwarding the message;

With the exception of 305 (Use Proxy) responses, the IBCF shall not recurse on 3xx responses.

### 5.10.3.3 Subsequent requests

Upon receipt of a subsequent request, the IBCF shall:

- 1) if the request is an INVITE request, then respond with a 100 (Trying) provisional response;
  - 1A) if the request is a NOTIFY request with the Subscription-State header field set to "terminated" and the IBCF has retained the SIP dialog state information for the associated subscription, once the NOTIFY transaction is terminated, the IBCF can remove all the stored information related to the associated subscription;
- 2) if the request is a target refresh request and the IBCF is configured to perform application level gateway and/or transport plane control functionalities, then the IBCF shall save the Contact and CSeq header field values received in the request such that the IBCF is able to release the session if needed;
- 3) if the subsequent request is other than a target refresh request (including requests relating to an existing dialog where the method is unknown) and the IBCF is configured to perform application level gateway and/or transport plane control functionalities, then the IBCF shall save the Contact and CSeq header field values received in the request such that the IBCF is able to release the session if needed;
- 4) void; and
- 5) if the request is received from an untrusted domain, remove all Feature-Caps header fields, if present;

and forwards the request, based on the topmost Route header field, in accordance with the procedures of RFC 3261 [26].

### 5.10.3.4 IBCF-initiated call release

If the IBCF provides transport plane control functionality and receives an indication of a transport plane related error the IBCF may:

- 1) generate a BYE request for the terminating side based on information saved for the related dialog; and
- 2) generate a BYE request for the originating side based on the information saved for the related dialog.



NOTE: Transport plane related errors can be indicated from e.g. TrGW or PCRF. The protocol for indicating transport plane related errors to the IBCF is out of scope of this specification.

Upon receipt of the 2xx responses for both BYE requests, the IBCF shall release all information related to the dialog and the related multimedia session.

### 5.10.3.5 Abnormal cases

When the IBCF acting as an entry point in the home originating PLMN is unable to forward a SIP request, as determined by one of the following:

- there is no response to the SIP request and its retransmissions by the IBCF; or
- by unspecified means available to the IBCF;

and:

- the IBCF supports S-CSCF restoration procedures;

then the IBCF:

- 1) shall reject the request by returning a 504 (Server Time-out) response; and
- 2) shall include in the 504 (Server Time-out) response:
  - a Content-Type header field with the value set to associated MIME type of the 3GPP IM CN subsystem XML body as described in subclause 7.6.1;
  - a P-Asserted-Identity header field set to the value of the SIP URI of the IBCF included in the Path header field during the registration (see subclause 5.10.3.1); and
  - a 3GPP IM CN subsystem XML body containing:
    - a) an <ims-3gpp> element with the "version" attribute set to "1" and with an <alternative-service> child element, set to the parameters of the alternative service:
      - i) a <type> child element, set to "restoration" (see table 7.6.2) to indicate that restoration procedures are supported;
      - ii) a <reason> child element, set to an operator configurable reason; and
      - iii) an <action> child element, set to "initial-registration" (see table 7.6.3).

NOTE: These procedures do not prevent the usage of unspecified reliability or recovery techniques above and beyond those specified in this subclause.

## 5.10.4 THIG functionality in the IBCF

### 5.10.4.1 General

NOTE 1: THIG functionality is performed in I-CSCF in Release-5 and Release-6 and is compatible with the procedures specified in this subclause.

The following procedures shall only be applied if network topology hiding is required by the network. The network requiring network topology hiding is called the hiding network.

NOTE 2: Requests and responses are handled independently therefore no state information is needed for that purpose within an IBCF.

The IBCF shall apply network topology hiding to all header fields which reveal topology information, such as Via, Route, and Record-Route.

NOTE 3: If the P-CSCF is located in the visited network and in order to allow the subscription initiated by the P-CSCF to the user's registration-state event package, the IBCF cannot apply network topology hiding on the Path header field contained in the REGISTER request.

NOTE 4: In order to allow the roaming UE to perform restoration procedures when the S-CSCF rejects the served user initiated request, the IBCF cannot apply network topology hiding on the Service-Route header field contained in a 200 (OK) response for the REGISTER request.

Upon receiving an incoming REGISTER request for which network topology hiding has to be applied and which includes a Path header field, the IBCF shall add the routeable SIP URI of the IBCF to the top of the Path header field. The IBCF may include in the inserted SIP URI an indicator that identifies the direction of subsequent requests received by the IBCF i.e., from the S-CSCF towards the P-CSCF, to identify the UE-terminating case. The IBCF may encode this indicator in different ways, such as, e.g., a unique parameter in the URI, a character string in the username part of the URI, or a dedicated port number in the URI.

NOTE 5: Any subsequent request that includes the direction indicator (in the Route header field) or arrives at the dedicated port number, indicates that the request was sent by the S-CSCF towards the P-CSCF.

Upon receiving an incoming initial request for which network topology hiding has to be applied and which includes a Record-Route header field, the IBCF shall add its own routeable SIP URI to the top of the Record-Route header field.

#### 5.10.4.2 Encryption for network topology hiding

Upon receiving an outgoing request/response from the hiding network the IBCF shall perform the encryption for network topology hiding purposes, i.e. the IBCF shall:

- 1) use the whole header field values which were added by one or more specific entity of the hiding network as input to encryption, besides the UE entry;
- 2) not change the order of the header fields subject to encryption when performing encryption;
- 3) use for one encrypted string all received consecutive header field entries subject to encryption, regardless if they appear in separate consecutive header fields or if they are consecutive entries in a comma separated list in one header field;
- 4) construct a hostname that is the encrypted string;
- 5) append a "tokenized-by" header field parameter and set it to the value of the encrypting network's name, after the constructed hostname;
- 6) form one valid entry for the specific header field out of the resulting NAI, e.g. prepend "SIP/2.0/UDP" for Via header fields or "sip:" for Route and Record-Route header fields;
- 7) if the IBCF encrypted an entry in the Route header field, then it also inserts its own URI before the topmost encrypted entry; and
- 8) if the IBCF encrypted an entry in the Via header field, then it also inserts its own URI before the topmost encrypted entry.

NOTE 1: Even if consecutive entries of the same network in a specific header field are encrypted, they will result in only one encrypted header field entry. For example:

```
Via: SIP/2.0/UDP ibcf1.home1.net;lr,
      SIP/2.0/UDP Token( SIP/2.0/UDP scscf1.home1.net;lr,
                        SIP/2.0/UDP pcscf1.home1.net;lr);
                        tokenized-by=home1.net,
      SIP/2.0/UDP [5555::aaa:bbb:ccc:ddd]
```

NOTE 2: If multiple entries of the same network are within the same type of header fields, but they are not consecutive, then these entries will be tokenized to different strings. For example:

```
Record-Route: sip:ibcf1.home1.net;lr,
              sip:Token(sip:scscf1.home1.net;lr);tokenized-by=home1.net,
              sip:asl.foreign.net;lr,
              sip:Token(sip:scscf1.home1.net;lr,
                        sip:pcscf1.home1.net;lr);tokenized-by=home1.net
```

NOTE 3: If request will return to the hiding network (e.g. after visiting an AS), then the URI of IBCF is inserted. For example:

```
Route: sip:asl.foreign.net;lr,
      sip:ibcf1.home1.net;lr,
      sip:Token(sip:scscf1.home1.net;lr);tokenized-by=home1.net
```

### 5.10.4.3 Decryption for network topology hiding

Upon receiving and incoming requests/response to the hiding network the IBCF shall perform the decryption for network topology hiding purposes, i.e. the IBCF shall:

- 1) identify hostnames encrypted by the network this IBCF belongs to within all header fields of the incoming message;
- 2) use those hostnames that carry the identification of the hiding network within the value of the "tokenized-by" header field parameter as input to decryption;
- 3) use as encrypted string the hostname which follows the sent-protocol (for Via header fields, e.g. "SIP/2.0/UDP") or the URI scheme (for Route and Record-Route header fields, e.g. "sip:");
- 4) replace all content of the received header field which carries encrypted information with the entries resulting from decryption.

**EXAMPLE:** An encrypted entry to a Via header field that looks like:

```
Via: SIP/2.0/UDP Token(SIP/2.0/UDP scscf1.home1.net;lr,
      SIP/2.0/UDP pcscf1.home1.net;lr);tokenized-by=home1.net
```

will be replaced with the following entries:

```
Via: SIP/2.0/UDP scscf1.home1.net;lr, SIP/2.0/UDP pcscf1.home1.net;lr
```

**NOTE:** Motivations for these decryption procedures are e.g. to allow the correct routing of a response through the hiding network, to enable loop avoidance within the hiding network, or to allow the entities of the hiding network to change their entries within e.g. the Record-Route header field.

### 5.10.5 IMS-ALG functionality in the IBCF

The IBCF shall only apply the following procedures if application level gateway functionality is required by the network.

The IBCF acts as a B2BUA when it performs IMS-ALG functionality. As an IMS-ALG, the IBCF will internally map the message header fields between the two dialogs that it manages. It is responsible for correlating the dialog identifiers and will decide when to simply translate a message from one dialog to the other, or when to perform other functions. The IBCF, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

An IBCF may replace a contact address with a URI of its own when the contact address in the incoming message is not a GRUU. In all other cases the IBCF shall use a GRUU (e.g. when the contact address is an IP address).

The IBCF shall transparently forward a received Contact header field when the Contact header field contains a GRUU or a media feature tag is included indicating a capability for which the Contact URI can be used by the remote party. When transparently forwarding a received Contact header field of a dialog-forming request, the IBCF shall include its own URI in a Record-Route header field in order to ensure that it is included on the route of subsequent requests.

**NOTE:** One example of such a media feature tag is the isfocus media feature tag used by conference services to transport the temporary conference identity that can be used when rejoining an ongoing conference.

The internal function of the IBCF as an IMS-ALG is defined in 3GPP TS 29.162 [11A].

If the IBCF receives a message with a body part for a UE from an S-CSCF, and:

- if the body part is the 3GPP IM CN subsystem XML body (as indicated by the Content-Type header field, see subclause 7.6) and the body part is not optional (as indicated by the (absence of the) Content-Disposition header field); or
- if a header field that describes the body is present and the header field's value is not understood (e.g. Content-Language header field or Content-Encoding header field);

then the IBCF shall transparently forward the message with the body part and the header field(s) that describe the body part.

## 5.10.6 Screening of SIP signalling

### 5.10.6.1 General

The IBCF may act as a B2BUA when it performs screening of SIP signalling functionality. In this case the B2BUA behaviour of the IBCF shall comply with the description given in subclause 5.10.5 for the IMS-ALG functionality.

**NOTE:** Many header fields are intended for end-to-end operation; removal of such header fields will impact the intended end-to-end operation between the end users. Additionally the IM CN subsystem does not preclude security mechanisms covering SIP header fields; any such removal can prevent validation of all header fields covered by the security mechanism.

### 5.10.6.2 IBCF procedures for SIP header fields

If specified by local policy rules, the IBCF may omit or modify any received SIP header fields prior to forwarding SIP messages, with the following exceptions.

As a result of any screening policy adopted, the IBCF should not modify at least the following header fields which would cause misoperation of the IM CN subsystem:

- Authorization; and
- WWW-Authenticate.

Where the IBCF appears in the path between the UE and the S-CSCF, some header fields are involved in the registration and authentication of the user. As a result of any screening policy adopted as part of normal operation, e.g. where the request or response is forwarded on, the IBCF should not modify as part of the registration procedure at least the following header fields:

- Path; and
- Service-Route.

**NOTE 1:** If the IBCF modifies SIP information elements (SIP header fields, SIP message bodies) other than as specified by SIP procedures (e.g., RFC 3261 [26]) caution needs to be taken that SIP functionality (e.g., routing using Route, Record-Route and Via) is not impacted in a way that could create interoperability problems with networks that assume that this information is not modified.

**NOTE 2:** Where operator requirements can be achieved by configuration hiding, then these procedures can be used in preference to screening.

The IBCF may add, remove, or modify, the P-Early-Media header field within forwarded SIP requests and responses according to procedures in RFC 5009 [109].

**NOTE 3:** The IBCF can use the P-Early-Media header field for the gate control procedures, as described in 3GPP TS 29.214 [13D]. In the presence of early media for multiple dialogs due to forking, if the IBCF is able to identify the media associated with a dialog, (i.e., if symmetric RTP is used by the UE and the IBCF can use the remote SDP information to determine the source of the media) the IBCF can selectively open the gate corresponding to an authorized early media flow for the selected media.

The IBCF may add, or omit any P-Asserted-Identity header fields prior to forwarding SIP messages according to local policy.

**NOTE 4:** The IBCF can use the P-Asserted-Identity header field to trigger identity specific procedures in subsequent entities, e.g. for malicious call identification. As an example, a P-Asserted-Identity header field will be deleted and a new P-Asserted-Identity header field with operator specific content will be added to the outgoing request, if the request was received from a network which cannot support the deletion of INFO request which is needed for the support of the malicious call identification service.

When the IBCF, located in the home network, receives a SIP request from another entity within the same trust domain, the IBCF may police the ICSI value contained in the P-Asserted-Service header field.

### 5.10.6.3 IBCF procedures for SIP message bodies

If the IBCF acts as a B2BUA, and the IBCF receives a message with a body part for a UE from an S-CSCF, and:

- if the body part is the 3GPP IM CN subsystem XML body (as indicated by the Content-Type header field, see subclause 7.6) and the body part is not optional (as indicated by the (absence of the) Content-Disposition header field); or
- if a header field that describes the body is present and the header field's value is not understood (e.g. Content-Language header field or Content-Encoding header field),

then the IBCF shall transparently forward the message with the body part and the header field(s) that describe the body part.

If IP address translation (NA(P)T or IP version interworking) occurs on the user plane, the IBCF shall modify SDP according to subclause 6.7.1;

Additionally, the IBCF may take the followings action upon SIP message bodies:

- 1) examine the length of a SIP message body and if required by local policy, take an appropriate action (e.g. forward the message body transparently, reject the request, remove the body);
- 2) examine the characteristics of the SIP message body MIMEs (i.e. check the values of any Content-Type, Content-Disposition, and Content-Language header fields), take an appropriate action defined by local policy (e.g. forward the body unchanged, remove the SIP message body MIME, reject the call); and
- 3) examine the content of SIP message body MIMEs, and take appropriate action defined by local policy (e.g. forward the body unchanged, remove the SIP message body MIME, reject the call).

When the intended action of an IBCF, based on local policy, is to remove a message body MIME from a SIP message body, and a Content-Disposition header field with a "handling" parameter set to "required" is associated with the MIME, the IBCF shall reject the SIP request with the 415 (Unsupported Media Type) response code as specified in RFC 5621 [150].

## 5.10.7 Media transcoding control

### 5.10.7.1 General

The IBCF may perform the media transcoding control in order to allow establishing communication between IM CN subsystems using different media codecs based on the interworking agreement and session information. When performing media transcoding control the IBCF acts as a special case of an IMS-ALG compliant with the description given in subclause 5.10.5.

### 5.10.7.2 Media transcoding control procedures

Upon receipt of any request containing an SDP offer, based on local policy and signalling inspection (e.g ICSI values, SDP), the IBCF may perform media transcoding control. Based on the local configuration determines the media which requires transcoding in the SDP offer.

Before forwarding the request to the answerer, the IBCF may add to the selected media one or more codecs at the end of the codec list contained in the SDP in order to give priority to the codecs inserted by the offerer over the codecs inserted by the IBCF. The codecs added to the offer are based on local policy.

NOTE 1: There is no mechanism to indicate to the terminating UE which codecs have been inserted by the network. However, RFC 4566 [39] recommends to list codecs in priority order, so by adding network inserted codecs to the end of the codec list will give higher priority to previous codecs that might have been inserted by the originating UE.

Upon receipt of any response containing an SDP answer, the IBCF shall inspect the list of the returned codecs and proceed as follows:

- if the list contains at least one of the codecs belonging to the original offer, the IBCF shall not invoke the transcoding function; and

- if the list contains none of the codecs belonging to the original offer, the IBCF shall select one of the returned codecs introduced in the answer and invoke the transcoding function. In order to perform the transcoding the IBCF shall select one of the codecs originally offered and set to a non-zero port value the related media stream in the answer sent to the offerer.

NOTE 2: The protocol used between IBCF and TrGW to allow the transport plane media transcoding control is out of scope of this specification. The codec selected by the answerer and the one selected by the IBCF and sent to the offerer can be used to instruct the TrGW for the transcoding purposes.

The IBCF shall remove from the SDP the codecs added to the original offer before forwarding the response to the offerer.

NOTE 3: In accordance with normal SDP procedure the transcoding IBCF informs the answerer of the properties of the chosen codecs (IP-address and ports).

### 5.10.8 Privacy protection at the trust domain boundary

In order to ensure privacy IBCF shall additionally to what is specified in subclause 4.4 and before sending the SIP requests or SIP responses outside the trust domain boundary perform the privacy protection as specified in RFC 3323 [33] and RFC 4244 [66] applicable to header fields with the clarifications in this subclause. If there are any conflicts between topology hiding specified in subclause 5.10.4 and the procedures in this subclause, the topology hiding takes precedence over privacy protection.

If a Privacy header field with a value different from "none" is received the IBCF shall:

- 1) if "header" privacy is requested as specified in RFC 3323 [33]:
  - remove all received Via header fields and then add a single Via header field with a URI of its own as described in RFC 3323 [33] subclause 5.1;
  - if the Contact header field does not contain a GRUU or does not contain an isfocus media feature tag, replace the value of the URI of the Contact header field with a URI that does not dereference to the originator of the message as described in RFC 3323 [33] subclause 5.1;
  - remove any Record-Route header fields as described in RFC 3323 [33] subclause 5.1; and
  - according to local policy either remove the History-Info header field or anonymize each entry in the History-Info header field;
- 2) if "user" level privacy is requested as specified in RFC 3323 [33]:
  - anonymize the From header field. The convention for configuring an anonymous From header field described in RFC 3323 [33] and RFC 3325 [34] should be followed; i.e. From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag= xxxxxxx;
- 3) if "history" privacy is requested in the Privacy header field as specified in RFC 4244 [66] according to local policy either remove the History-Info header field or anonymize each entry in the History-Info header field;
- 4) if privacy is requested within the History-Info header field as specified in RFC 4244 [66] according to local policy either remove or anonymize every entry that contains the privacy parameter "history"; and
- 5) if any modification of any dialog-matching headers for privacy protection reasons is done act as a transparent B2BUA as described in RFC 3323 [33] subclause 5.3.

If a Privacy header field is not received IBCF may based on local policy act as if "id", "user", "header" and "history" was received and perform privacy protection as specified in RFC 3325 [34], RFC 3323 [33] and RFC 4244 [66] with the clarifications above.

If a Privacy header field with the value "none" is received the IBCF should not protect the privacy of the identity information.

NOTE: A local policy can regard a Privacy header field with the value "none" the same as if no Privacy header field was received.

## 5.10.9 Roaming architecture for voice over IMS with local breakout

The IBCF shall apply OMR as specified in 3GPP TS 29.079 [11D] and in accordance with the roaming architecture for voice over IMS with local breakout when a session is identified as a roaming architecture for voice over IMS with local breakout session.

A session can be identified as a roaming architecture for voice over IMS with local breakout session when a received initial INVITE request contains a Feature-Caps header field with a "+g.3gpp.trf" header field parameter, a "+g.3gpp.loopback" header field parameter or any other implementation dependent indication.

NOTE: An implementation dependent indication can e.g. be in a URI parameter, a character string in the user part of the URI or be a port number in the URI.

## 5.11 Procedures at the E-CSCF

### 5.11.1 General

The PSAP may either be directly connected to the IM CN subsystem or via the PSTN.

The E-CSCF can receive URIs for a domain for which the operator running the E-CSCF is not responsible. Where RFC 3261 [26] specifies a requirement that the SIP entity has to be responsible for the domain for particular functionality to occur, the E-CSCF may ignore this restriction.

NOTE 1: The E-CSCF would normally implement this override if the P-CSCF or S-CSCF is configured to pass on URIs (e.g. Request-URI) that are outside the responsible domain of the E-CSCF, otherwise emergency calls might not be routed to a PSAP. If the P-CSCF or S-CSCF does not do this, then the override need not be applied.

The E-CSCF retrieves a PSAP URI, based on the location of the UE and the requested type of emergency service. The PSAP URI can be retrieved from LRF (see subclause 5.11.3) or from local configuration. The PSAP address will either point to a PSAP connected to the IM CN subsystem or to a PSAP connected to the PSTN.

If operator policy determines that the E-CSCF selects the PSAP and if, based on the location information contained in the INVITE request, the E-CSCF fails to select the PSAP, the E-CSCF can interrogate an external server in order to retrieve location information.

NOTE 2: The protocol used between an E-CSCF and an external server is not specified in this version of the specification.

When the E-CSCF receives an emergency request for a dialog requesting privacy or a standalone emergency transaction requesting privacy or any request or response related to a UE-originated emergency dialog requesting privacy, and if operator policy (e.g. determined by national regulatory requirements applicable to emergency services) allows requests for suppression of public user identifiers and location information per 3GPP TS 22.101 [1A], the E-CSCF:

- shall provide the privacy service role according to RFC 3323 [33] and RFC 3325 [34];

NOTE 3: The procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34] and subclause 4.4.

- shall remove any location object from the message's body with Content-Type header field containing the content type application/pidf+xml. If only one message body remains in the message's body then the E-CSCF sets the Content-Type header field to the content type specified for the body; and
- shall remove the Geolocation header field (if present) and the Geolocation-Routing header field (if present);

prior to forwarding any such request to a PSAP.

NOTE 4: If the routing functions are supported by an LRF, this information is not removed before the request is sent to the LRF.

### 5.11.2 UE originating case

The E-CSCF may either forward an emergency request to a PSAP in the IP network or forward the request to a PSAP in the PSTN. In the latter case the request will pass a BGCF and a MGCF before entering the PSTN.

Upon receipt of an initial request for a dialog, or a standalone transaction, or an unknown method including a Request-URI with an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69], or an emergency number the E-CSCF shall:

1) if:

- a) the topmost Route header field of the received SIP INVITE request contains an E-CSCF URI inserted by a P-CSCF, an AS or an IBCF;

NOTE 1: The E-CSCF is identified by two URIs, one preconfigured in the P-CSCF, AS or IBCF and one used to receive the request from EATF.

- b) the Contact header field includes an instance-id feature tag containing an IMEI URN as specified in RFC 7254 [153] or an MEID URN as specified in RFC 8464 [187]. Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks; and

- c) required by the operator policy;

then:

a0) remove its own SIP URI from the topmost Route header field;

- a) insert URI of the EATF to be contacted into the Route header field as the topmost entry followed by own URI to be used to receive the request from EATF;
- b) insert a type 3 "orig-ioi" header field parameter in the P-Charging-Vector header field. The E-CSCF shall set the type 3 "orig-ioi" header field parameter to a value that identifies the sending network of the request. The E-CSCF shall not include the type 3 "term-ioi" header field parameter;

- c) if required by national regulatory requirements applicable to emergency services, include:

- a CPC with value "emergency"; and optionally
- an OLI set to a value corresponding to the characteristics of the access used when the emergency request was initiated by the UE, i.e., an OLI that corresponds to a wireless access; and

- d) route the request based on SIP routing procedures and do not continue with the rest of the steps;

1A) remove its own SIP URI from the topmost Route header field;

1B) if the received request does not contain an ICID in a P-Charging-Vector header field, insert a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17];

1C) if an "orig-ioi" header field parameter is received in the P-Charging-Vector header field, store the value of the received "orig-ioi" header field parameter;

NOTE 2: Any received "orig-ioi" header field parameter will be a type 2 IOI generated by an S-CSCF or passed on by an IBCF. The type 2 IOI identifies the network from which the request was sent.

1D) if operator policy determines that an LRF is to be used, forward the request to the LRF as indicated in subclause 5.11.3;

- 2) if the PSAP is the next hop, store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field and remove the received information in the P-Charging-Vector header field, else keep the P-Charging-Vector if the next hop is an exit IBCF or a BGCF;
- 3) if the PSAP is the next hop remove the P-Charging-Function-Addresses header fields, if present, else keep the P-Charging-Function-Addresses header fields if the next hop is an exit IBCF or a BGCF;
- 4) if an IBCF or a BGCF is the next hop, delete any received "orig-ioi" header field parameter, and insert a type 2 "orig-ioi" header field parameter into the P-Charging-Vector header field. The E-CSCF shall set the type 2 "orig-ioi" header field parameter to a value that identifies the sending network. The E-CSCF shall not include the "term-ioi" header field parameter;

5) get location information as:



- geographical location information received in a PIDF location object [90], with the content type application/pidf+xml, as described RFC 6442 [89]; and
- location identifier as derived from the P-Access-Network-Info header field, if available.

NOTE 3: As an alternative to retrieve location information from the LRF the E-CSCF can also request location information from an external server. The address to the external server can be received in the Geolocation header field as specified in RFC 6442 [89]. The protocol used to retrieve the location information from the external server is not specified in this version of the specification.

5A) if the location is retrieved using information from the Geolocation header field, and if:

- the Geolocation-Routing header field is present, and includes a value not allowing routing of the request based on user location information;
- the Geolocation-Routing header field is present, and includes a value unknown to the E-CSCF; or
- the Geolocation-Routing header field is not present.

not use the location retrieved from the Geolocation header field when deciding where to forward the request.

6) select, based on location information and optionally type of emergency service:

- a) a PSAP connected to the IM CN subsystem and add the PSAP URI to the topmost Route header field; or

NOTE 4: If the user did not request privacy or if national regulator policy applicable to emergency services does not require the user be allowed to request privacy, the E-CSCF conveys the Geolocation header field (if present), the Geolocation-Routing header field (if present), the location information in a PIDF location object (if present) and the P-Access-Network-Info header field containing the location identifier, if defined for the access type as specified in subclause 7.2A.4, to the PSAP.

- b) a PSAP in the PSTN, add the BGCF URI to the topmost Route header field, add a PSAP URI in tel URI format to the Request-URI with an entry used in the PSTN/CS domain to address the PSAP and set the handling header field parameter value of the Content-Disposition header field associated with the application/pidf+xml message body (if present) to "optional";

NOTE 5: If the user did not request privacy or if national regulator policy applicable to emergency services does not require the user be allowed to request privacy, the E-CSCF conveys the Geolocation header field (if present), the Geolocation-Routing header field (if present), the location information in a PIDF location object (if present) and the P-Access-Network-Info header field containing the location identifier, if defined for the access type as specified in subclause 7.2A.4, towards the MGCF. The MGCF can translate the location information if included in INVITE (i.e. both the geographical location information in PIDF-LO and the location identifier in the P-Access-Network-Info header field) into ISUP signalling, see 3GPP TS 29.163 [11B].

NOTE 6: The way the E-CSCF determines the next hop address when the PSAP address is a tel URI is implementation dependent.

7) void;

8) if due to local policy or if the PSAP requires interconnect functionalities (e.g. PSAP address is of an IP address type other than the IP address type used in the IM CN subsystem), put the address of the IBCF to the topmost Route header field, in order to forward the request to the PSAP via an IBCF in the same network;

9) create a Record-Route header field containing its own SIP URI;

10) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the E-CSCF is able to release the session if needed; and

11) if no P-Asserted-Identity header field is present and if required by operator policy governing the indication to PSAPs that a UE does not have sufficient credentials (e.g. determined by national regulatory requirements applicable to emergency services), insert a P-Asserted-Identity header field set to a non-dialable callback number (see ANSI/J-STD-036-B [176]);

NOTE 7: A P-Asserted-Identity header field that is present can contain a reference number used in the communication between the PSAP and LRF according to procedures in subclause 5.11.3. Such a P-Asserted-Identity header field would not be replaced with a P-Asserted-Identity header field set to a non-dialable callback number.

12) if required by national regulatory requirements applicable to emergency services, include:

- a CPC with value "emergency"; and optionally
- an OLI set to a value corresponding to the characteristics of the access used when the emergency request was initiated by the UE, i.e., an OLI that corresponds to a wireless access; and

13) route the request based on SIP routing procedures.

NOTE 8: Depending on local operator policy, the E-CSCF has the capability to reject requests relating to specific methods in accordance with RFC 3261 [26], as an alternative to the functionality described above.

Upon receipt of an initial request for a dialog, a standalone transaction, or an unknown method, that does not include a Request-URI with an emergency service URN or an emergency number, the E-CSCF shall reject the request by sending a 403 (Forbidden) response.

When the E-CSCF receives the request containing the access-network-charging-info parameter in the P-Charging-Vector, the E-CSCF shall store the access-network-charging-info parameter from the P-Charging-Vector header field. The E-CSCF shall retain access-network-charging-info parameter in the P-Charging-Vector header field.

When the E-CSCF receives any request or response (excluding ACK requests and CANCEL requests and responses) related to a UE-originated dialog or standalone transaction, the E-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses header fields before forwarding the message. If the original request contained a P-Charging-Vector header field including an orig-IOI header field parameter, insert a type 2 "term-ioi" header field parameter in the P-Charging-Vector header field of the outgoing response. The type 2 "term-ioi" header field is set to a value that identifies the sending network of the response and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter. Values of "orig-ioi" and "term-ioi" header field parameters in the received response are removed.

When the E-CSCF receives any 1xx or 2xx response related to a UE-originated dialog or standalone transaction, the E-CSCF shall remove any P-Preferred-Identity header field and P-Asserted-Identity header field, and insert a P-Asserted-Identity header field with the digits that can be recognized as a valid emergency number if dialled as a tel URI representing the number, before forwarding the message.

NOTE 9: Numbers that can be recognized as valid emergency numbers if dialled by the user are specified in 3GPP TS 22.101 [1A]. The emergency numbers 112 and 911 are stored on the ME, in accordance with 3GPP TS 22.101 [1A].

When the E-CSCF receives any response related to a UE-originated dialog or standalone transaction containing a "term-ioi" header field parameter, the E-CSCF shall store the value of the received "term-ioi" header field parameter received in the P-Charging-Vector header field, if present, and remove all received "orig-ioi" and "term-ioi" header field parameters.

NOTE 10: Any received "term-ioi" header field parameter will be a type 2 IOI. The IOI identifies the sending network of the response message.

When the E-CSCF receives an INVITE request from the UE, the E-CSCF may require the periodic refreshment of the session to avoid hung states in the E-CSCF. If the E-CSCF requires the session to be refreshed, the E-CSCF shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 11: Requesting the session to be refreshed requires support by at least the UE or the PSAP or MGCF. This functionality cannot automatically be granted, i.e. at least one of the involved UAs needs to support it in order to make it work.

### 5.11.3 Use of an LRF

Where the network operator determines that an LRF is to be used, the E-CSCF shall route initial requests for a dialog and standalone requests that contain an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69], or an emergency number, to the LRF in accordance with the procedures of RFC 3261 [26].

NOTE 1: The E-CSCF is by definition responsible for emergency service URNs and is therefore allowed to change the Request-URI of requests containing emergency service URNs when a 3xx or 416 response is received.

For the outgoing request, the E-CSCF shall:

- 1) insert a type 3 "orig-ioi" header field parameter in the P-Charging-Vector header field. The E-CSCF shall set the type 3 "orig-ioi" header field parameter to a value that identifies the sending network of the request. The E-CSCF shall not include the type 3 "term-ioi" header field parameter.

When the E-CSCF receives any 3xx response to such a request, the E-CSCF shall select a Contact header field URI from the 3xx response according to RFC 3261 [26] and continue processing the steps given in subclause 5.11.2 with the following additions:

- a) at step 6), if item a) applies, place the URI received in the selected Contact header field URI in the 3xx response in the topmost entry in the Route header field;
- b) at step 6), if item b) applies, replace the original Request-URI with the URI received in the selected Contact header field URI in the 3xx response;
- c) if the user did not request privacy or if national regulator policy applicable to emergency services does not require the user be allowed to request privacy, then if the selected Contact header field URI contains a P-Asserted-Identity header field encoded as a header field of the URI, replace all P-Asserted-Identity header fields in the original request with this value;

NOTE 2: Such a P-Asserted-Identity header field contains a reference number which is used in the communication between the PSAP and LRF.

- d) if operator local policies allow insertion of UE location information and if the received 3xx response contains a message/external-body MIME type as specified in RFC 4483 [186] with "access-type" MIME type parameter containing "URL" and "URL" MIME type parameter containing an HTTP or HTTPS URI identifying a PIDF location object as defined in RFC 4119 [90], then the E-CSCF shall insert a Geolocation header field containing this PIDF location object by reference (see RFC 6442 [89]); and
- e) if operator policies allows forming requests from a URI and if 3xx response is received, then follow the procedures of RFC 3261 [26] subclause 19.1.5 with the following additions and clarifications:
  - replacement or inclusion of any header field from the URI in the selected Contact header field is subject to operator policy; and
  - if operator policy allows any LRF to provide a location by value, and the URI in the selected Contact header field contains the "Geolocation" header field, a "Geolocation-Routing" header field and a header field with hname "body" with a value, replace the entire message body with value of the header field with hname "body" in the URI in the selected Contact header field, otherwise do not perform this replacement.

If no 1xx or 2xx response to the request is received from the addressed PSAP within an operator settable timeout, or a 4xx – 5xx response is received, and additional URI values were included in the Contact header field of the response, the E-CSCF shall use these values according to RFC 3261 [26] in new requests that are otherwise generated according to the rules specified above.

If no 1xx or 2xx response to the request is received from the addressed PSAP within an operator settable timeout, or a 4xx – 5xx response is received, and all URI values included in the Contact header field of the 3xx response have been attempted, the E-CSCF shall use a default URI value configured in the E-CSCF in a new request that is otherwise generated according to the rules specified above.

If a 6xx response to the request is received, the E-CSCF acts in accordance with RFC 3261 [26].

When the E-CSCF receives any response related to the above request containing a "term-ioi" header field parameter, the E-CSCF shall store the value of the received "term-ioi" header field parameter received in the P-Charging-Vector header field, if present, and remove all received "orig-ioi" and "term-ioi" header field parameters from the forwarded response.

NOTE 3: Any received "term-ioi" header field parameter will be a type 3 IOI. The IOI identifies the sending network of the response message.

If no 3xx response to the request is received from the LRF within an operator settable timeout, the E-CSCF shall use a default URI value configured in the E-CSCF in a request that is otherwise generated according to the rules specified above.

## 5.11.4 Subscriptions to E-CSCF events

### 5.11.4.1 Subscription to the event providing dialog state

When an incoming SUBSCRIBE request addressed to the E-CSCF arrives containing the Event header field with the dialog event package, the E-CSCF shall:

- 1) based on the local policy, check if the request was generated by a subscriber who is authorised to subscribe to the registration state of this particular user. The authorized subscribers include:
  - all the LRFs that belong to the same network operator.

If the requester is not authorised, the E-CSCF shall reject the request with an appropriate 4xx – 6xx response;

- 2) store the value of the "orig-ioi" header field parameter received in the P-Charging-Vector header field if present; and

NOTE: Any received "orig-ioi" header field parameter will be a type 3 IOI. The type 3 IOI identifies the service provider from which the request was sent.

- 3) generate a 2xx response acknowledging the SUBSCRIBE request and indicating that the authorised subscription was successful as described in RFC 4235 [171]. The E-CSCF shall populate the header fields as follows:
  - an Expires header field, set to either the same or a decreased value as the Expires header field in the SUBSCRIBE request; and
  - a P-Charging-Vector header field containing the "orig-ioi" header field parameter, if received in the SUBSCRIBE request, and a type 3 "term-ioi" header field parameter. The E-CSCF shall set the type 3 "term-ioi" header field parameter to a value that identifies the sending network of the response and the "orig-ioi" header field parameter is set to the previously received value of the "orig-ioi" header field parameter.

The E-CSCF may set the Contact header field to an identifier uniquely associated to the SUBSCRIBE request and generated within the E-CSCF, that may help the E-CSCF to correlate refreshes for the SUBSCRIBE.

Afterwards the E-CSCF shall perform the procedures for notification about dialog state as described in subclause 5.11.4.2.

When the E-CSCF receives a subscription refresh request for a dialog that was established by the UE subscribing to the dialog event package, the E-CSCF shall accept the request.

### 5.11.4.2 Notification about dialog state

The E-CSCF shall send a NOTIFY request when an event pertaining to the dialog or dialogs occurs, as specified in RFC 3265 [28].

When generating NOTIFY requests, the E-CSCF shall not preclude any valid dialog event package parameters in accordance with RFC 4235 [171]. Where RFC 4235 [171] expresses an option or only a recommendation as to the generation of a NOTIFY request, it is a matter of operator policy as to whether such requests are generated.

For each NOTIFY request triggered by an event and on all dialogs which have been established due to subscription to the dialog event package, and in addition to the requirements specified in RFC 4235 [171], the E-CSCF shall:

- 1) set the P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17], and a type 3 "orig-ioi" header field parameter. The E-CSCF shall set the type 3 "orig-ioi" header field parameter to a value that identifies the sending network of the request. The E-CSCF shall not include the type 3 "term-ioi" header field parameter.
- 2) in the body of the NOTIFY request, include one <dialog> XML element for each dialog to be reported in accordance with the subscription; and
- 3) for each <dialog> XML element:

- if the subscription is for all dialogs, rather than a specific dialog, then include the call-id attribute.

If the subscription is to a specific dialog (or to a specific set of dialogs), when sending a final NOTIFY request with all dialogs set to a state of "terminated", the E-CSCF shall also terminate the subscription to the dialog event package by setting the Subscription-State header field to the value of "terminated".

When the E-CSCF receives any response to the NOTIFY request, the E-CSCF shall store the value of the "term-ioi" header field parameter received in the P-Charging-Vector header field, if present.

NOTE: Any received "term-ioi" header field parameter will be a type 3 IOI. The type 3 IOI identifies the service provider from which the response was sent.

## 5.12 Location Retrieval Function (LRF)

### 5.12.1 General

The LRF can receive URIs for a domain for which the operator running the LRF is not responsible. Where RFC 3261 [26] specifies a requirement that the SIP entity has to be responsible for the domain for particular functionality to occur, the LRF may ignore this restriction.

NOTE: The LRF would normally implement this override if the P-CSCF is configured to pass on URIs (e.g. Request-URI) that are outside the responsible domain of the LRF, otherwise emergency calls might not be routed to a PSAP. If the P-CSCF does not do this, then the override need not be applied.

### 5.12.2 Treatment of incoming initial requests for a dialog and standalone requests

The LRF shall respond to all received initial requests for a dialog, and to all standalone requests, as a redirect server as defined in subclause 8.3 of RFC 3261 [26] with the following additions:

- 1) the LRF shall generate a 300 (Multiple Choices) response to all such requests;
- 2) the LRF shall set the Contact header field of the response to a list (one or more) address(es) of PSAP(s), selected according to network operator policy;

NOTE 1: The mechanisms for selection of PSAP addresses are outside the scope of this specification, but can be based on a variety of input information including the value of the URN included in the Request-URI of the request, the value of the Geolocation header field and Geolocation-Routing header field received in the request, the value of the P-Access-Network-Info header field received in the request, any location known at the LRF for the requesting user as identified by the P-Access-Network-Info header field.

- 2A) if the location is retrieved using information from the Geolocation header field, and if:
  - the Geolocation-Routing header field is present, and includes a value not allowing routing of the request based on user location information;
  - the Geolocation-Routing header field is present, and includes a value unknown to the LRF; or
  - the Geolocation-Routing header field is not present;

the LRF shall not use the location retrieved from the Geolocation header field when selecting PSAP(s);

- 3) the LRF shall insert a P-Charging-Vector header field containing the "orig-ioi" header field parameter, if received in the request and a type 3 "term-ioi" header field parameter. The LRF shall set the type 3 "term-ioi" header field parameter to a value that identifies the service provider from which the response is sent and the "orig-ioi" header field parameter is set to the previously received value of "orig-ioi" header field parameter;
- 4) optionally, generate a reference identifier and set the P-Asserted-Identity header field encoded as a header field of the URI in the Contact header field to this value in each included Contact header field URI associated with a PSAP. The LRF shall maintain state for any generated reference identifier. If the LRF uses a SIP URI (or any other permitted URI scheme other than tel URI) as the reference identifier, the LRF has the responsibility of ensuring (e.g. by configuration) that the emergency request is being routed to an IP connected PSAP. Subclause 5.12.3.1 defines a means of maintaining the state of the reference identifier. If required by operator policy governing the indication to PSAPs that a UE does not have sufficient credentials (e.g. determined by

national regulatory requirements applicable to emergency services), the reference identifier shall not be equal to a non-dialable callback number used to indicate the UE does not have credentials;

NOTE 2: The reference identifier is used to correlate information requested over the Le interface (see 3GPP TS 23.167 [4B]) and is not needed if the Le interface is not used. The protocol at the Le interface is not defined in this release.

NOTE 3: The reference identifier is managed by the RDF or the LRF. If the RDF manages the reference identifier, the LRF obtains the a reference identifier from the RDF. In some regional systems, this reference identifier is the ESQK.

5) if required by operator local policies, the LRF shall include a message/external-body MIME type as specified in RFC 4483 [186] with:

a) "access-type" MIME type parameter containing "URL"; and

b) "URL" MIME type parameter containing an HTTP or HTTPS URI identifying a PIDF location object as defined in RFC 4119 [90]; and

6) if required by operator local policies, the LRF shall include geographical information, encoded as header fields of the URI in a Contact header field of the 300 (Multiple Choices) response, in the following way:

a) if operator policy indicates location-by-reference is to be used:

i. a Geolocation-Routing header field with value "yes"; and

ii. a Geolocation header field that contains an HTTP URI or a HTTPS URI associated with a location-by-reference, as defined in RFC 6442 [89]; and

b) if operator policy indicates location-by-value is to be used:

i. a Geolocation-Routing header field with value "yes";

ii. Geolocation header field with value associated with the location-by-value;

iii. a header field with hname "body" and with a value that contains an escape encoded MIME body of multipart/mixed MIME type containing:

- the MIME body from the received request; and

- the geographical location information as PIDF location object in accordance with RFC 4119 [90]; and

iv. a Content-Type header field with multipart/mixed MIME type.

NOTE 4: The mechanisms for selection of PSAP addresses are outside the scope of this specification. See note 1.

NOTE 5: The body of the received request can include a PIDF location object and SDP.

## 5.12.3 Subscription and notification

### 5.12.3.1 Notification about dialog state

Based on operator policy, the LRF can either subscribe to all dialog information on an E-CSCF or individually subscribe to each dialog as it receives the requests.

NOTE 1: Subscription to dialog information is dependent on the use of Le interface as described in subclause 5.12.2.

In the case that the LRF is subscribing to all dialogs at the E-CSCF, the LRF shall generate a SUBSCRIBE request to the dialog state event package in accordance with RFC 3265 [28] and RFC 4235 [171]. The LRF shall include the following additional information in the SUBSCRIBE request:

a) the Request-URI set to an E-CSCF address;

NOTE 2: In this case, it is expected that the LRF will be configured with a set of E-CSCF addresses, and the LRF will subscribe to all of them.

- b) no header field parameters in the Event header field;
- c) an Expires header field set to 600 000 seconds; and
- d) a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17] and a type 3 "orig-ioi" header field parameter. The type 3 "orig-ioi" header field parameter identifies the service provider from which the request is sent. The LRF shall not include the type 3 "term-ioi" header field parameter.

Upon generation of a 300 response to an incoming dialog forming request that contains a reference identifier, and in the case that the LRF is subscribing to individual dialogs at the E-CSCF, the LRF shall generate a SUBSCRIBE request to the dialog state event package in accordance with RFC 3265 [28] and RFC 4235 [171]. The LRF shall include the following additional information in the SUBSCRIBE request:

- a) the Request-URI set to the value of the P-Asserted-Identity in the original request to which the response was generated;
- b) a Route header field that addresses the request to the E-CSCF. How such a value is determined depends on deployment;

NOTE 3: A number of mechanisms exist for identifying the required E-CSCF, however all suffer some restrictions. It is therefore a matter of configuration at deployment time to identify the solution that works for that particular deployment. Mechanisms that exist include:

- i) if there is only one E-CSCF in the network, using the address of that E-CSCF preconfigured into the system;
  - ii) using the last entry in the Via header field of the original request to which the 3xx response was generated. If the deployment however includes some intermediate SIP proxy or B2BUA not otherwise included in the emergency call architecture this will not provide the desired result; or
  - iii) using the IP address from which the original request was received to which the 3xx response was generated. The request is sent to the same port number and IP address as the 3xx response was generated. If the deployment however includes some intermediate SIP proxy or B2BUA not otherwise included in the emergency call architecture this will not provide the desired result, and additionally, if the system is set up to use port numbers in a unidirectional manner, i.e. one port number for requests and another port number for responses, it will also not operate correctly.
- c) the "call-id" and "to-tag" header field parameters in the Event header field set to the values in the original request to which the 3xx response was generated. No "from-tag" header field parameter can be included as it is not known by the LRF;
  - d) an Expires header field set to 86400 seconds; and
  - ) a P-Charging-Vector header field with the "icid-value" header field parameter populated as specified in 3GPP TS 32.260 [17] and a type 3 "orig-ioi" header field parameter. The type 3 "orig-ioi" header field parameter identifies the service provider from which the request is sent. The LRF shall not include the type 3 "term-ioi" header field parameter.

In the case that the LRF is subscribing to individual dialogs at the E-CSCF, and a NOTIFY request is received indicating a state of "terminated", the LRF shall end the subscription to the dialog event package.

NOTE 4: Such NOTIFY requests will normally be accompanied by the Subscription-State header field set to the value of "terminated".

When, as a result of successful subscription to the dialog event package, the LRF receives a notification containing dialog updates, the LRF shall update its record for each dialog included in the event package information.

## 5.13 ISC gateway function

### 5.13.1 General

As specified in 3GPP TS 23.218 [5] border control functions may be applied between the IM CN subsystem and an application server based on operator preference. The ISC gateway function may act both as an entry point and as an exit point for a network. If it processes a SIP request received from another network it functions as an entry point (see

subclause 5.13.3) and it acts as an exit point whenever it processes a SIP request sent to other network (see subclause 5.13.2).

In many cases, the ISC interface carries more than one hop of the session, e.g.. the application server has applied a service to a SIP request and then returned the SIP request to the S-CSCF, or a AS acting as a third-party call controller generates multiple outgoing legs. In these cases all the requests relating to the session on all hops / legs should be configured to route through the same ISC gateway function.

NOTE 1: This is to provide for future requirements for the ISC gateway function that may need to provide correlation of the SIP transactions, and additional functionality based on that correlation.

This ISC gateway function exists on a one to one basis with its addressed AS, i.e. the URI used to address the ISC gateway function will always reach the same AS beyond the ISC gateway function.

The functionalities of the ISC gateway function are entry and exit point procedures as defined in subclause 5.13.2 and subclause 5.13.3 and additionally can include:

- network configuration hiding (as defined in subclause 5.13.4);
- application level gateway (as defined in subclause 5.13.5);
- transport plane control, i.e. QoS control (as defined in subclause 5.13.5); and
- screening of SIP signalling (as defined in subclause 5.13.6);

NOTE 2: The functionalities performed by the application level gateway are configured by the operator, and it is network specific.

## 5.13.2 ISC gateway function as an exit point

### 5.13.2.1 Registration

There are no specific requirements for the REGISTER method, i.e. the REGISTER method is treated as for other SIP methods.

### 5.13.2.2 General

This subclause applies for requests sent from the S-CSCF to the AS via the ISC gateway function.

For all SIP transactions identified:

- if priority is supported, as containing an authorised Resource-Priority header field or a temporarily authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field, the ISC gateway function shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs.

NOTE: The special treatment can include filtering, higher priority processing, routing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

### 5.13.2.3 Initial requests

Upon receipt of:

- an initial request for a dialog;
- a request for a standalone transaction; or
- a request for an unknown method that does not relate to an existing dialog;

the ISC gateway function shall:

- 1) if the request is an INVITE request, respond with a 100 (Trying) provisional response;
- 2) remove the topmost entry from the Route header field in accordance with RFC 3261 [26] procedures for processing Route header fields, and then add as the topmost entry the URI of the application server associated



with this ISC gateway function, followed by a next entry of a URI needed to reach this ISC gateway function from the application server;

- 3) if the request is an INVITE request and the ISC gateway function is configured to perform application level gateway and/or transport plane control functionalities, save the Contact, CSeq and Record-Route header field values received in the request such that the ISC gateway function is able to release the session if needed;
- 4) If the request is a SUBSCRIBE and the ISC gateway function does not need to act as B2BUA, based on operator policy, the ISC gateway function shall determine whether or not to retain, for the related subscription, the SIP dialog state information and the duration information;

NOTE 1: The event package name can be taken into account to decide whether or not the SIP dialog state and the subscription duration information needs to be retained.

NOTE 2: The ISC gateway function needs to insert its own URI in the Record-Route header field of the SUBSCRIBE request if it decides to retain the SIP dialog state information.

- 5) if the request is an initial request for a dialog and local policy requires the application of ISC gateway function capabilities in subsequent requests, perform record route procedures as specified in RFC 3261 [26];
- 6) if the recipient of the request is understood from configured information to always send and receive private network traffic from this source, remove the P-Private-Network-Indication header field containing the domain name associated with that saved information;
- 7) store the values from the P-Charging-Function-Addresses header field, if present;
- 8) remove some of the parameters from the P-Charging-Vector header field or the header field itself, depending on operator policy, if present; and
- 9) remove the P-Charging-Function-Addresses header fields, if present, prior to forwarding the message;

and forwards the request according to RFC 3261 [26].

NOTE 3: If ISC gateway function processes a request without a pre-defined route (e.g. the subscription to reg event package originated by the AS), the next-hop address can be either obtained as specified in RFC 3263 [27A] or be provisioned in the ISC gateway function.

When the ISC gateway function receives an INVITE request, the ISC gateway function may require the periodic refreshment of the session to avoid hung states in the ISC gateway function. If the ISC gateway function requires the session to be refreshed, the ISC gateway function shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 4: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

When the ISC gateway function receives a response to any of the requests handled in this subclause, then the ISC gateway function shall:

- 1) in the P-Charging-Vector header field, subject to operator policy, reinsert any parameters that were removed and stored. In addition, where the operator policy requires it, include on behalf of the supported application server a type 3 "term-ioi" header field parameter. This IOI may represent either the network of the ISC gateway function or the network providing the AS.

With the exception of 305 (Use Proxy) responses, the ISC gateway function shall not recurse on 3xx responses.

#### 5.13.2.4 Subsequent requests

Upon receipt of a subsequent request, the ISC gateway function shall:

- 1) if the request is an INVITE request, respond with a 100 (Trying) provisional response;
- 2) if the request is a NOTIFY request with the Subscription-State header field set to "terminated" and the ISC gateway function has retained the SIP dialog state information for the associated subscription, once the NOTIFY transaction is terminated, the ISC gateway function can remove all the stored information related to the associated subscription;

- 3) if the request is a target refresh request and the ISC gateway function is configured to perform application level gateway and/or transport plane control functionalities, save the Contact and CSeq header field values received in the request such that the ISC gateway function is able to release the session if needed; and
- 4) if the subsequent request is other than a target refresh request (including requests relating to an existing dialog where the method is unknown) and the ISC gateway function is configured to perform application level gateway and/or transport plane control functionalities, save the Contact and CSeq header field values received in the request such that the ISC gateway function is able to release the session if needed;

and forwards the request, based on the topmost Route header field, in accordance with the procedures of RFC 3261 [26].

### 5.13.2.5 Call release initiated by ISC gateway function

If the ISC gateway function provides transport plane control functionality and receives an indication of a transport plane related error the ISC gateway function may:

- 1) generate a BYE request for the terminating side based on information saved for the related dialog; and
- 2) generate a BYE request for the originating side based on the information saved for the related dialog.

NOTE: Transport plane related errors can be indicated from e.g. TrGW. The protocol for indicating transport plane related errors to the ISC gateway function is out of scope of this specification.

Upon receipt of the 2xx responses for both BYE requests, the ISC gateway function shall release all information related to the dialog and the related multimedia session.

## 5.13.3 ISC gateway function as an entry point

### 5.13.3.1 Registration

There are no specific requirements for the REGISTER method, i.e. the REGISTER method is treated as for other SIP methods.

### 5.13.3.2 General

This subclause applies for requests sent from the AS to the S-CSCF via the ISC gateway function. Such requests come from the AS as a result of a request received from the S-CSCF and forwarded by the the ISC gateway function.

For all SIP transactions identified:

- if priority is supported (NOTE), as containing an authorised Resource-Priority header field or a temporarily authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field, the ISC gateway function shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs.

NOTE: The special treatment can include filtering, higher priority processing, routing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

### 5.13.3.3 Initial requests

Upon receipt of:

- an initial request for a dialog;
- a request for a standalone transaction; or
- a request for an unknown method that does not relate to an existing dialog;

the ISC gateway function shall verify whether the request is arrived from a trusted domain or not. If the request arrived from an untrusted domain, then the ISC gateway function shall:

- remove all P-Charging-Vector header fields and all P-Charging-Function-Addresses header fields the request may contain.

Upon receipt of:

- an initial request for a dialog;
- a request for a standalone transaction except the REGISTER request; or
- a request for an unknown method that does not relate to an existing dialog;

the ISC gateway function shall:

- 1) if the request is an INVITE request, respond with a 100 (Trying) provisional response;
- 2) remove the topmost entry from the Route header field in accordance with RFC 3261 [26] procedures for processing Route header fields;
- 3) if a P-Private-Network-Indication header field is included in the request, check whether the configured information allows the receipt of private network traffic from this source. If private network traffic is allowed, the ISC gateway function shall check whether the received domain name in any included P-Private-Network-Indication header field in the request is the same as the domain name associated with that configured information. If private network traffic is not allowed, or the received domain name does not match, then the ISC gateway function shall remove the P-Private-Network-Indication header field;
- 4) if the initiator of the request is understood from configured information to always send and receive private network traffic from this source, insert a P-Private-Network-Indication header field containing the domain name associated with that configured information;
- 5) if the request is an INVITE request and the ISC gateway function is configured to perform application level gateway and/or transport plane control functionalities, then the ISC gateway function shall save the Contact, CSeq and Record-Route header field values received in the request such that the ISC gateway function is able to release the session if needed;
- 6) If the request is a SUBSCRIBE and the ISC gateway function does not need to act as B2BUA, based on operator policy, the ISC gateway function shall determine whether or not to retain, for the related subscription, the SIP dialog state information and the duration information; and

NOTE 1: The event package name can be taken into account to decide whether or not the SIP dialog state and the subscription duration information needs to be retained.

NOTE 2: The ISC gateway function needs to insert its own URI in the Record-Route header field of the SUBSCRIBE request if it decides to retain the SIP dialog state information.

- 7) if the request is an initial request for a dialog and local policy requires the application of ISC gateway function capabilities in subsequent requests, perform record route procedures as specified in RFC 3261 [26];

When the ISC gateway function receives an INVITE request, the ISC gateway function may require the periodic refreshment of the session to avoid hung states in the ISC gateway function. If the ISC gateway function requires the session to be refreshed, the ISC gateway function shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 3: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

When the ISC gateway function receives a response to an initial request (e.g. 183 or 2xx), the ISC gateway function shall:

- 1) store the values from the P-Charging-Function-Addresses header field, if present; and
- 2) remove the P-Charging-Function-Addresses header field prior to forwarding the message.

With the exception of 305 (Use Proxy) responses, the ISC gateway function shall not recurse on 3xx responses.

### 5.13.3.4 Subsequent requests

Upon receipt of a subsequent request, the ISC gateway function shall:

- 1) if the request is an INVITE request, then respond with a 100 (Trying) provisional response;

- 2) if the request is a NOTIFY request with the Subscription-State header field set to "terminated" and the ISC gateway function has retained the SIP dialog state information for the associated subscription, once the NOTIFY transaction is terminated, the ISC gateway function can remove all the stored information related to the associated subscription;
- 3) if the request is a target refresh request and the ISC gateway function is configured to perform application level gateway and/or transport plane control functionalities, then the ISC gateway function shall save the Contact and CSeq header field values received in the request such that the ISC gateway function is able to release the session if needed; and
- 4) if the subsequent request is other than a target refresh request (including requests relating to an existing dialog where the method is unknown) and the ISC gateway function is configured to perform application level gateway and/or transport plane control functionalities, then the ISC gateway function shall save the Contact and CSeq header field values received in the request such that the ISC gateway function is able to release the session if needed;

and forwards the request, based on the topmost Route header field, in accordance with the procedures of RFC 3261 [26].

### 5.13.3.5 Call release initiated by the ISC gateway function

If the ISC gateway function provides transport plane control functionality and receives an indication of a transport plane related error the ISC gateway function may:

- 1) generate a BYE request for the terminating side based on information saved for the related dialog; and
- 2) generate a BYE request for the originating side based on the information saved for the related dialog.

NOTE: Transport plane related errors can be indicated from e.g. TrGW. The protocol for indicating transport plane related errors to the ISC gateway function is out of scope of this specification.

Upon receipt of the 2xx responses for both BYE requests, the ISC gateway function shall release all information related to the dialog and the related multimedia session.

### 5.13.4 THIG functionality in the ISC gateway function

The ISC gateway function shall act according to the procedures defined for the IBCF in subclause 5.10.4 with the following exceptions:

- there are no specific requirements for the REGISTER method, i.e. the REGISTER method is treated as for other SIP methods.

### 5.13.5 IMS-ALG functionality in the ISC gateway function

The ISC gateway function shall act according to the procedures defined for the IBCF in subclause 5.10.5.

### 5.13.6 Screening of SIP signalling

The ISC gateway function shall act according to the procedures defined for the IBCF in subclause 5.10.6.

NOTE 1: Subclause 5.10.6 identifies a number of header fields that should not be screened. It is not expected that the ISC gateway function will see these header fields.

NOTE 2: In identifying header fields to be screened, care is needed to ensure that header fields needed by application servers later in the filter criteria chain are not removed. The ordering of the applications in the filter criteria chain might be reordered if this is a constraint that cannot be met.

## 6 Application usage of SDP

### 6.1 Procedures at the UE

#### 6.1.1 General

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 [30] as updated by RFC 4032 [64].

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect SDP message bodies. Hence, the UE shall not encrypt SDP message bodies.

During the session establishment procedure, and during session modification procedures, SIP messages shall only contain an SDP message body if that is intended to modify the session description, or when the SDP message body is included in the message because of SIP rules described in RFC 3261 [26].

NOTE 1: A codec can have multiple payload type numbers associated with it.

In order to support accurate bandwidth calculations, the UE may include the "a=ptime" attribute for all "audio" media lines as described in RFC 4566 [39]. If a UE receives an "audio" media line with "a=ptime" specified, the UE should transmit at the specified packetization rate. If a UE receives an "audio" media line which does not have "a=ptime" specified or the UE does not support the "a=ptime" attribute, the UE should transmit at the default codec packetization rate as defined in RFC 3551 [55A]. The UE will transmit consistent with the resources available from the network.

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

For "video" and "audio" media types that utilize the RTP/RTCP, in addition to the "b=AS" parameter, the UE may specify the "b=TIAS", and "a=maxprate" parameters in accordance with RFC 3890 [152]. The value of the parameter shall be determined as described in RFC 3890 [152]. The value or absence of the "b=" parameter(s) may affect the assigned QoS which is defined in 3GPP TS 29.213 [13C].

If a UE receives a media line which contains both a=ptime and a=maxprate, the UE should use the a=maxprate value, if this attribute is supported.

If multiple codecs are specified on the media line, "a=maxprate" (or "a=ptime" if "a=maxprate" is not available or not supported) should be used to derive the packetization time used for all codecs specified on the media line. Given that not all codecs support identical ranges of packetization, the UE should ensure that the packetization derived by "a=maxprate" (or "a=ptime" if "a=maxprate" is not available or not supported) is a valid packetization time for each codec specified in the list.

If the media line in the SDP message body indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556 [56], then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 [56] to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890 [152].

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in or 3GPP 29.213 [13C].

NOTE 2: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

If an in-band DTMF codec is supported by the application associated with an audio media stream, then the UE shall include, in addition to the payload type numbers associated with the audio codecs for the media stream, for each clock rate associated with the audio codecs for the media stream, a payload type number associated with the MIME subtype "telephone-event", to indicate support of in-band DTMF as described in RFC 4733 [23].

The UE shall inspect the SDP message body contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 [54] and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

In case of UE initiated resource reservation and if the UE determines resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 3: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

In order to fulfil the QoS requirements of one or more media streams, the UE may re-use previously reserved resources. In this case the UE shall indicate as met the local preconditions related to the media stream, for which resources are re-used.

If the SDP is affected due to a rejected IP-CAN bearer, a modified IP-CAN bearer or a released IP-CAN bearer then the UE shall:

- 1) update the session according to RFC 3261 [26] and RFC 3311 [29] and set the ports of the media stream(s) for which IP-CAN resource was rejected, modified or released to zero in the new SDP offer;
- 2) release the session according to RFC 3261 [26];
- 3) cancel the session setup or the session modification according to RFC 3261 [26]; or
- 4) reject the session setup or the session modification according to RFC 3261 [26].

NOTE 4: The UE can use one IP address for signalling (and specify it in the Contact header field) and different IP address(es) for media (and specify it in the "c=" parameter of the SDP).

If the UE wants to transport media streams with TCP and there are no specific alternative negotiation mechanisms defined for that particular application, then the UE shall support the procedures and the SDP rules specified in RFC 4145 [83].

## 6.1.2 Handling of SDP at the originating UE

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the SDP offer, the UE:

- shall indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1);
- shall set the related media streams to inactive, by including an "a=inactive" line, according to the procedures described in RFC 4566 [39], unless the UE knows that the precondition mechanism is supported by the remote UE; and
- if the UE supports the precondition mechanism (see subclause 5.1.3.1), shall not request confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE.

NOTE 1: When setting the media streams to the inactive mode, the UE can include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

If the UE supports the precondition mechanism (see subclause 5.1.3.1), and the desired QoS resources for one or more media streams are available at the UE when the SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment and shall not request confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE.

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in the SDP message body.

If the UE indicated support for end-to-access-edge security during registration, and the P-CSCF indicated support for end-to-access-edge security during registration, then upon generating an SDP offer for media plane security containing

an SDES crypto attribute as defined in RFC 4568 [168], the UE shall include the SDES crypto attribute according to the profile defined in 3GPP TS 33.328 [19C] and an SDP attribute "a=3ge2ae:requested" for all media with the following exceptions:

- a) media transported by a protocol with no supported media security mechanism; and

NOTE 3: This release of this document supports only media security mechanisms for RTP based media.

- b) media for which the UE requests an end-to-end security mechanism.

If the P-CSCF did not indicate support for end-to-access-edge security during registration, the UE shall not include an attribute "a=3ge2ae:requested" in any SDP offer.

When the UE detects that an emergency call is being made, the UE shall not include end-to-end media security on any media in the SDP offer.

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the SDP offer shall contain a subset of the allowed media types, codecs and other parameters from the SDP message bodies of all 488 (Not Acceptable Here) responses so far received for the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). For each media line, the UE shall order the codecs in the SDP offer according to the order of the codecs in the SDP message bodies of the 488 (Not Acceptable Here) responses.

NOTE 4: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP message bodies of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Upon confirming successful local resource reservation, the UE shall create an SDP offer in which:

- the related local preconditions are set to met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64]; and
- the media streams previously set to inactive mode are set to active (sendrecv, sendonly or recvonly) mode.

Upon receiving an SDP answer, which includes more than one codec per media stream, excluding the in-band DTMF codec, as described in subclause 6.1.1, the UE shall send an SDP offer at the first possible time, selecting only one codec per media stream.

If the UE sends an initial INVITE request that includes only an IPv6 address in the SDP offer, and receives an error response (e.g., 488 (Not Acceptable Here) with 301 Warning header field) indicating "incompatible network address format", the UE shall send an ACK as per standard SIP procedures. Subsequently, the UE may acquire an IPv4 address or use an existing IPv4 address, and send a new initial INVITE request to the same destination containing only the IPv4 address in the SDP offer.

### 6.1.3 Handling of SDP at the terminating UE

Upon receipt of an initial SDP offer in which no precondition information is available, the terminating UE shall in the SDP answer:

- if, prior to sending the SDP answer the desired QoS resources have been reserved at the terminating UE, set the related media streams in the SDP answer to:
  - active mode, if the offered media streams were not listed as inactive; or
  - inactive mode, if the offered media streams were listed as inactive.

If the terminating UE had previously set one or more media streams to inactive mode and the QoS resources for those media streams are now ready, the UE shall set the media streams to active mode by applying the procedures described in RFC 4566 [39] with respect to setting the direction of media streams.

Upon sending a SDP answer to an SDP offer (which included one or more media lines which was offered with several codecs) the terminating UE shall select exactly one codec per media line and indicate only the selected codec for the

related media stream. In addition, the UE may indicate support of the in-band DTMF codec, as described in subclause 6.1.1.

Upon sending a SDP answer to an SDP offer, with the SDP answer including one or more media streams for which the originating side did indicate its local preconditions as not met, if the precondition mechanism is supported by the terminating UE, the terminating UE shall indicate its local preconditions and request the confirmation for the result of the resource reservation at the originating end point.

NOTE 1: If the terminating UE does not support the precondition mechanism it will ignore any precondition information received from the originating UE.

Upon receiving an initial INVITE request, that includes the SDP offer containing an IP address type (in the "c=" parameter) that is not supported by the UE, the UE shall respond with the 488 (Not Acceptable Here) response with 301 Warning header field indicating "incompatible network address format".

NOTE 2: Upon receiving an initial INVITE request that does not include an SDP offer, the UE can accept the request and include an SDP offer in the first reliable response. The SDP offer will reflect the called user's terminal capabilities and user preferences for the session.

If the UE receives an SDP offer that specifies different IP address type for media (i.e. specify it in the "c=" parameter of the SDP offer) that the UE is using for signalling, and if the UE supports both IPv4 and IPv6 addresses simultaneously, the UE shall accept the received SDP offer. Subsequently, the UE shall either acquire an IP address type or use an existing IP address type as specified in the SDP offer, and include it in the "c=" parameter in the SDP answer.

NOTE 3: Upon receiving an initial INVITE request, that includes an SDP offer containing connection addresses (in the "c=" parameter) equal to zero, the UE will select the media streams that is willing to accept for the session, reserve the QoS resources for accepted media streams, and include its valid connection address in the SDP answer.

Upon receiving an initial INVITE request, that includes an SDP offer containing an SDES crypto attribute as defined in RFC 4568 [168] and indicating that the P-CSCF has applied e2ae-security to the media plane (i.e. "a=3ge2ae:applied") the UE shall:

- 1) proceed with the session setup as described in this subclause and indicating media plane security using SDES as defined in RFC 4568 [168], implementing the SDES crypto attribute according to the profile defined in 3GPP TS 33.328 [19C]; or
- 2) act based on local policy (local policy can e.g. cause the UE to reject the incoming call, or to trigger user interaction).

If the terminating UE uses the precondition mechanism (see subclause 5.1.4.1), if the desired QoS resources for one or more media streams have not been reserved at the terminating UE when constructing the SDP offer, the terminating UE shall indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment.

NOTE 4: It is out of scope of this specification which media streams are to be included in the SDP offer.

If the terminating UE uses the precondition mechanism (see subclause 5.1.4.1) and if the desired QoS resources for one or more media streams are available at the terminating UE when the SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment.

If the terminating UE sends an UPDATE request to remove one or more media streams negotiated in the session for which a final response to the INVITE request has not been sent yet, the terminating UE sets the ports of the media streams to be removed from the session to zero in the new SDP offer.

## 6.2 Procedures at the P-CSCF

The P-CSCF shall perform IMS-ALG functionality:

- when the P-CSCF needs to perform procedures for hosted NAT traversal according to Annex F; or
- when the P-CSCF needs to perform procedures for media plane security (see subclause 6.7.2.2);



- when required by the user-related policies provisioned to the P-CSCF (see subclause 5.2.1);
- when the P-CSCF needs to perform ECN procedures (see subclause 6.7.2.3);
- when the P-CSCF needs to perform procedures for OMR (see subclause 6.7.2.4);
- when the P-CSCF needs to perform P-CSCF controlled NA(P)T and NA(P)T-PT (see subclause 6.7.2.5);
- when the P-CSCF needs to perform hosted NAT procedures (see subclause 6.7.2.6);
- when the P-CSCF needs to perform ICE procedures (see subclause 6.7.2.7); or
- when the P-CSCF needs to perform transcoding procedures (see subclause 6.7.2.8).

When the P-CSCF receives any SIP request containing an SDP offer, the P-CSCF shall examine the media parameters in the received SDP offer.

If the P-CSCF finds any media parameters which are not allowed on the network by local policy or if available by bandwidth authorisation limitation information coming from the IP-CAN (e.g. via PCRF), the P-CSCF shall return a 488 (Not Acceptable Here) response containing an SDP message body. This SDP message body contains either all the media types, codecs and other SDP parameters which are allowed according to the local policy, or, based on configuration by the operator of the P-CSCF, a subset of these allowed parameters. This subset may depend on the content of the received SIP request. For each media line, the P-CSCF shall build the SDP message body in the 488 (Not Acceptable Here) response in the same manner as a UAS builds the SDP message body in a 488 (Not Acceptable Here) response as specified in RFC 3261 [26]. The P-CSCF shall order the codecs with the most preferred codec listed first. If the SDP offer is encrypted, the P-CSCF may reject the request.

Subject to local policy, if it is not possible to generate a SDP message body (e.g. the available bandwidth is less than the bandwidth of any codec allowed by the local policy), the P-CSCF shall return a 486 (Busy here) response with a 370 Warning header field indicating "insufficient bandwidth".

When the P-CSCF receives a SIP response different from 200 (OK) response containing SDP offer, the P-CSCF shall not examine the media parameters in the received SDP offer, but the P-CSCF shall rather check the succeeding request containing the SDP answer for this offer, and if necessary (i.e. the SDP answer reduced by the UE still breaches local policy, or if available by bandwidth authorisation limitation information coming from the IP-CAN, e.g. via PCRF), the P-CSCF shall return a 488 (Not Acceptable Here) response containing the local policy allowed SDP message body. If the SDP answer is encrypted, the P-CSCF may reject the succeeding request.

When the P-CSCF receives a 200 (OK) response containing SDP offer, the P-CSCF shall examine the media parameters in the received SDP offer. If the P-CSCF finds any media parameters which are not allowed on the network by local policy or if available by bandwidth authorisation limitation information coming from the IP-CAN (e.g. via PCRF), the P-CSCF shall forward the SDP offer and on the receipt of the ACK request containing the SDP answer, the P-CSCF shall immediately terminate the session as described in subclause 5.2.8.1.2. If the SDP offer is encrypted, the P-CSCF shall forward the SDP offer and on the receipt of the ACK request containing the SDP answer, it may immediately terminate the session as described in subclause 5.2.8.1.2.

In case a device performing address and/or port number conversions is provided by a NA(P)T or NA(P)T-PT controlled by the P-CSCF, or by a hosted NAT, the P-CSCF may need to modify the media connection data in SDP message bodies according to the procedures described in annex F or subclause 6.7.2.5.

The P-CSCF shall apply the same SDP policy to the initial request or response containing an SDP message body, and throughout the complete SIP session.

The P-CSCF may inspect, if present, the "b=RS" and "b=RR" lines in order to find out the bandwidth allocation requirements for RTCP.

Subject to local policy, the P-CSCF shall prohibit the negotiation of ECN during SDP offer/answer exchanges associated with multimedia priority service by removing any ECN attribute "a=ecn-capable-rtp" from the SDP offer and shall not invoke ECN for SIP transactions associated with multimedia priority service.

Additional procedures where the P-CSCF acts as an IMS-ALG are given in subclause 6.7.2. The IMS-ALG only applies where there are specific gateway capabilities to be provided.

## 6.3 Procedures at the S-CSCF

When the S-CSCF receives any SIP request containing an SDP offer, the S-CSCF shall examine the media parameters in the received SDP offer. If the S-CSCF finds any media parameters which are not allowed based on local policy or subscription (i.e. the information in the instances of the Core Network Service Authorization class in the service profile, described in 3GPP TS 29.228 [14]), the S-CSCF shall return a 488 (Not Acceptable Here) response containing an SDP message body. This SDP message body contains either all the media types, codecs and other SDP parameters which are allowed according to the local policy and users subscription or, based on configuration by the operator of the S-CSCF, a subset of these allowed parameters. This subset may depend on the content of the received SIP request. The S-CSCF shall build the SDP message body in the 488 (Not Acceptable Here) response in the same manner as a UAS builds the SDP message body in a 488 (Not Acceptable Here) response as specified in RFC 3261 [26]. If the SDP offer is encrypted, the S-CSCF may reject the request.

When the S-CSCF receives a SIP response different from 200 (OK) response containing SDP offer, the S-CSCF shall not examine the media parameters in the received SDP offer, but the S-CSCF shall rather check the succeeding request containing the SDP answer for this offer, and if necessary (i.e. the SDP answer reduced by the UE still breaches local policy), the S-CSCF shall return a 488 (Not Acceptable Here) response containing the local policy allowed SDP message body. If the SDP answer is encrypted, the S-CSCF may reject the succeeding request.

When the S-CSCF receives a 200 (OK) response containing an SDP offer, the S-CSCF shall examine the media parameters in the received SDP offer. If the S-CSCF finds any media parameters which are not allowed based on local policy or subscription (i.e. the information in the instances of the Core Network Service Authorization class in the service profile, described in 3GPP TS 29.228 [14]), the S-CSCF shall forward the SDP offer and on the receipt of the ACK request containing the SDP answer, the S-CSCF shall immediately terminate the session as described in subclause 5.4.5.1.2. If the SDP offer is encrypted, the S-CSCF shall forward the SDP offer and on the receipt of the ACK request containing the SDP answer, it may immediately terminate the session as described in subclause 5.4.5.1.2.

## 6.4 Procedures at the MGCF

### 6.4.1 Calls originating from circuit-switched networks

The usage of SDP by the MGCF is the same as its usage by the UE, as defined in the subclause 6.1 and A.3.2, with the following exceptions:

- in an initial SDP offer the MGCF shall not use the "inactive" attribute when the local preconditions are met;
- if local preconditions are not met at the MGCF and local configuration indicates that the MGCF is serving users not supporting SIP preconditions, then the MGCF shall set the inactive mode (by including an attribute "a=inactive") in an initial SDP offer, (otherwise all served users support the SIP preconditions and the inactive indication is not needed);
- in an initial INVITE request generated by a MGCF, the MGCF shall indicate the current status of the local precondition; and
- end-to-access edge security is not applicable to the MGCF.

When sending an SDP message body, the MGCF shall not include the "i=", "u=", "e=", "p=", "r=", and "z=" descriptors in the SDP message body, and the MGCF shall ignore them if received in an SDP message body.

When the MGCF generates and sends an INVITE request for a call originating in a circuit-switched network, the MGCF shall populate the SDP with the codecs supported by the associated MGW.

### 6.4.2 Calls terminating in circuit-switched networks

The usage of SDP by the MGCF is the same as its usage by the UE, as defined in the subclause 6.1 and A.3.2, with the following exceptions:

- a) when the MGCF sends a 183 (Session Progress) response with an SDP message body, the MGCF shall only request confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the originating end point if all of the following conditions are true:
  - there are any remaining unfulfilled preconditions at the originating end point;

- the received initial INVITE request indicates support of SIP preconditions; and
- local configuration indicates support of SIP preconditions; and

b) end-to-access edge security is not applicable to the MGCF.

When sending an SDP message body, the MGCF shall not include the "i=", "u=", "e=", "p=", "r=", and "z=" descriptors in the SDP message body, and the MGCF shall ignore them if received in an SDP message body.

### 6.4.3 Optimal Media Routeing (OMR)

If the MGCF supports OMR it shall also perform the UA procedures described in 3GPP TS 29.079 [11D].

### 6.4.4 Explicit congestion control support in MGCF

An MGW associated with an MGCF can support Explicit Congestion Notification (ECN) according to RFC 3168 [189], and can act as an ECN endpoint to enable ECN with a local ECN-capable terminal within a local network that properly handles ECN-marked packets.

If the MGCF receives a SDP offer containing ECN attribute "a=ecn-capable-rtp" as specified in RFC 6679 [188], and if the MGCF knows via configuration that the MGW handles ECN-marked packets properly then the MGCF, taking into account the initialisation method the MGW supports, shall return a SDP answer containing the ECN attribute "a=ecn-capable-rtp" according to RFC 6679 [188].

NOTE 1: The "leap" initialisation method is the only initialisation method the MGW supports over the Mn interface in this release.

When creating an SDP offer and if the MGCF knows via configuration that the MGW handles ECN-marked packets properly the MGCF may initiate ECN negotiation in accordance with RFC 6679 [188].

If the MGCF receives the SDP answer also containing ECN attribute "a=ecn-capable-rtp" then the MGCF will instruct the MGW to apply ECN procedures.

## 6.5 Procedures at the MRFC

Void.

## 6.6 Procedures at the AS

Since an AS may provide a wide range of different services, procedures for the SDP usage for an AS acting as originating UA, terminating UA or third-party call control role are dependent on the service provided to the UA and on the capabilities on the remote UA. There is no special requirements regarding the usage of the SDP, except the requirements for the SDP capabilities described in the following paragraphs and clause A.3:

- 1) Providing that an INVITE request generated by an AS contains an SDP message body, the AS has the capability of reflecting the originating AS's capabilities, desired QoS and precondition requirements for the session in the SDP message body.
- 2) When the AS sends a 183 (Session Progress) response with an SDP message body including one or more "m=" media types, it has the capability of requesting confirmation for the result of the resource reservation at the originating endpoint.

When an AS acts as a B2BUA, and it controls media resources using an MRF, it may support OMR. When the AS supports OMR, and it controls media resources using an MRF, it shall also perform the procedures described in 3GPP TS 29.079 [11D].

## 6.7 Procedures at the IMS-ALG functionality

### 6.7.1 IMS-ALG in IBCF

#### 6.7.1.1 General

When the IBCF acts as an IMS-ALG, it makes procedures as for an originating UA and terminating UA. The IMS-ALG acts as a B2BUA. The general treatment of the SDP information between originating UA and terminating UA is described in 3GPP TS 29.162 [11A]. For the use of the IMS-ALG for specific capabilities, additional procedures are defined in subsequent subclauses.

Subject to local policy, the IBCF shall prohibit the negotiation of ECN during SDP offer/answer exchanges associated with multimedia priority service by removing any ECN attribute "a=ecn-capable-rtp" from the SDP offer and shall not invoke ECN for SIP transactions associated with multimedia priority service.

NOTE: Disabling ECN in an IBCF does not prevent a P-CSCF (IMS ALG), subject to roaming agreement, from applying ECN over the access network between a UE and the P-CSCF (IMS-ALG).

#### 6.7.1.2 IMS-ALG in IBCF for support of ICE

##### 6.7.1.2.1 General

This subclause describes procedures of an IBCF to support ICE as defined in RFC 5245 [99].

If no TrGW is inserted, an IBCF may transparently pass ICE related SDP attributes to support ICE. The remaining procedures in this subclause are only applicable if the IBCF is inserting a TrGW on the media plane.

When the IBCF with attached TrGW receives SDP candidate information from the SDP offerer the IBCF shall not forward the candidate information towards the SDP answerer. When the IBCF receives SDP candidate information from the SDP answerer the IBCF shall not forward the candidate information towards the SDP offerer. The remaining procedures in this subclause are optional.

NOTE: An IBCF that removes and/or does not provide ICE related SDP attributes (e.g. a=candidate) in the offer/answer exchange will cause the ICE procedures to be aborted and the address and port information in the m and c lines of the SDP offer will be used. If this address and port information contains the relayed candidate address of a STUN Relay server, as recommended by ICE, then an extra media relay server will be used for the session which is not necessary nor desirable.

The IBCF with attached TrGW performs separate ICE procedures towards the SDP offerer and the SDP answerer. The usage of ICE is negotiated separately with the SDP offerer and SDP answerer, and ICE may be applied independently at either side. Furthermore, the IBCF may be configured to apply ICE procedures only towards one network side, e.g. towards the IM CN subsystem it belongs to.

Since the IBCF is not located behind a NAT, it does not request the TrGW to generate keep-alive messages even when acting as a full ICE entity. The IBCF only requests the TrGW to terminate and generate STUN messages used for the candidate selection procedures.

Since the IBCF is not located behind a NAT the IBCF shall only include host candidates in SDP offers and answers generated by the IBCF.

##### 6.7.1.2.2 IBCF full ICE procedures for UDP based streams

###### 6.7.1.2.2.1 General

This subclause describes the IBCF full ICE procedures for UDP based streams.

###### 6.7.1.2.2.2 IBCF receiving SDP offer

When the IBCF receives an SDP offer including ICE candidate information, the IBCF shall send the candidate information for each UDP based stream received in the SDP offer towards the TrGW. The IBCF will request the TrGW to reserve media- and STUN resources towards the SDP offerer, based on the candidate information, in order to allow the TrGW to perform the necessary connectivity checks per the ICE procedures.

If the SDP offerer is acting as an ICE controller entity the IBCF shall act as an ICE controlled entity in the direction towards the SDP offerer. If the SDP offerer is acting as an ICE controlled entity the IBCF shall act as an ICE controller entity in the direction towards the SDP offerer.

#### 6.7.1.2.2.3 IBCF sending SDP offer

Prior to sending an SDP offer, the IBCF may choose to apply related ICE procedures, e.g. if it expects to interact with terminals applying procedures as described in subclause K.5.2, and if both the IBCF and TrGW also support ICE procedures. To invoke these ICE procedures, the IBCF will request the TrGW to reserve media- and STUN resources towards the SDP answerer for each UDP based media stream and include a host candidate attribute for each UDP based stream in the SDP offer, providing the reserved address and port at the TrGW as destination.

The IBCF shall always act as an ICE controller entity towards the SDP answerer.

NOTE: The host candidate address included by the IBCF in the generated SDP offer matches the c- and m line information for the associated UDP stream in the SDP offer.

#### 6.7.1.2.2.4 IBCF receiving SDP answer

When the IBCF receives an SDP answer including ICE candidate information, the IBCF will send the candidate information for each UDP based stream received in the SDP answer towards the TrGW.

The IBCF will request the TrGW to perform ICE candidate selection procedures towards the SDP answerer. The IBCF will request the TrGW to inform the IBCF, for each UDP stream, which candidate pair has been selected towards the SDP answerer, once the candidate selection procedure towards the SDP answerer has finished.

If the TrGW indicates to the IBCF that, for at least one UDP stream, the selected candidate pair does not match the c- and m- line address information for the associated UDP stream, exchanged between the IBCF and the SDP answerer, and the IBCF acts as an ICE controller entity towards the SDP answerer, the IBCF shall send a new offer towards the SDP answerer in order to align the c- and m- lines address information with the chosen candidate pair for the associated UDP stream.

#### 6.7.1.2.2.5 IBCF sending SDP answer

When the IBCF generates an SDP answer for an offer that included ICE candidate information, the IBCF will request the TrGW to reserve media- and STUN resources towards the SDP offerer for each UDP based media stream and include an SDP host candidate attribute for each UDP based stream in the SDP answer, providing the reserved address and port at the TrGW as destination.

The IBCF shall in the generated SDP answer include host candidate information which matches the c- and m line information for the associated UDP stream in the SDP answer.

The IBCF will request the TrGW to perform ICE candidate selection procedures towards the SDP offerer. The IBCF will request the TrGW to inform the IBCF, for each UDP stream, which candidate pair has been selected towards the SDP offerer, once the candidate selection procedure towards the SDP offerer has finished.

If the TrGW indicates to the IBCF that the selected candidate pair towards the SDP offerer does not match the c- and m- line address information for the associated UDP stream, exchanged between the IBCF and the SDP offerer, and the IBCF acts as an ICE controller entity towards the SDP offerer, the IBCF shall send an offer towards the SDP offerer (which will now act as an SDP answerer) in order to align the c- and m- line address information with the chosen candidate pair for the associated UDP stream.

#### 6.7.1.2.3 IBCF ICE lite procedures for UDP based streams

When the IBCF is using ICE lite procedures for UDP based streams, the IBCF procedures are identical as described in subclause 6.7.1.2.2, with the following exceptions:

- The IBCF always acts as an ICE controlled entity towards the SDP offerer and towards the SDP answerer, and;
- The IBCF requests the TrGW to perform ICE lite candidate selection procedures, as defined in ICE

#### 6.7.1.2.4 ICE procedures for TCP based streams

##### 6.7.1.2.4.1 General

The IBCF shall terminate ICE procedures for TCP based streams. Instead the IBCF will use the mechanism defined in RFC 4145 [83] for establishing TCP based streams, as defined in RFC 6544 [131].

An entity that supports ICE continues the ICE procedures for UDP based streams, even if no candidates are provided for TCP based streams.

NOTE: The IBCF ICE procedures for TCP based streams are identical no matter whether the IBCF uses full ICE- or ICE lite- procedures for UDP based streams.

##### 6.7.1.2.4.2 IBCF receiving SDP offer

When the IBCF receives an SDP offer, the IBCF shall ignore the candidate attributes for TCP based streams. The IBCF shall not send the candidate information for TCP based streams towards the TrGW.

##### 6.7.1.2.4.3 IBCF sending SDP offer

When the IBCF generates an SDP offer the IBCF shall include an "actpass" setup attribute, as defined in RFC 4145 [83], for each TCP based stream, which will cause the SDP answerer to initiate the TCP connections towards the TrGW. The IBCF shall not include any candidate attributes for TCP based streams in the SDP offer.

##### 6.7.1.2.4.4 IBCF receiving SDP answer

Since the IBCF does not include candidates in the SDP offer towards the SDP answerer, there are no ICE specific procedures when the IBCF receives an SDP answer.

NOTE: If the SDP answer contains candidate attributes for TCP based streams, the IBCF simply discards the candidate attributes.

##### 6.7.1.2.4.5 IBCF sending SDP answer

When the IBCF generates an SDP answer the IBCF shall include a "passive" setup attribute, as defined in RFC 4145 [83], for each TCP based stream, which will cause the SDP offerer to initiate the TCP connections towards the TrGW. The IBCF shall not include any candidate attributes for TCP based streams in the SDP answer.

### 6.7.2 IMS-ALG in P-CSCF

#### 6.7.2.1 General

This subclause specifies the general procedures for the support of SDP in IMS-ALG within the P-CSCF. For the use of the IMS-ALG for specific capabilities, additional procedures are defined in subsequent subclauses.

When the IMS-ALG receives an SDP offer, it shall create a new SDP offer, based the contents of the received SDP offer, modified according to procedures and policies associated with specific capabilities that the IMS-ALG is used for, according to capabilities supported by the IMS-AGW, and to provide the IP address and port information received by the IMS-AGW.

When the IMS-ALG receives an SDP answer, it shall create a new SDP answer, to respond to the originally received SDP offer, modified according to the same procedures and policies that were used to modify the SDP offer.

The P-CSCF may receive multiple provisional responses with an SDP answer due to forking of a request before the first final answer is received. For each SDP answer received in such subsequent provisional responses, the P-CSCF shall apply the procedure in this subclause.

After the session is established, it is possible for both ends of the session to change the media connection data for the session. When the P-CSCF receives a SDP offer/answer where port number(s) or IP address(es) is/are included, there are three different possibilities:

- IP address(es) or/and port number(s) have been added;
- IP address(es) and port number(s) have been reassigned to the end points; or

NOTE 1: If necessary, the P-CSCF will request the IMS-AGW access gateway to release the resources related to the previously assigned IP address(es) and port number(s).

- no change has been made to the IP address(es) and port number(s).

NOTE 2: In the particular case of RTP flows, port conversions also apply to the associated RTCP flows.

### 6.7.2.2 IMS-ALG in P-CSCF for media plane security

When the P-CSCF acts as an IMS-ALG, it acts as a B2BUA and modifies the SDP as described as described in 3GPP TS 23.334 [7F].

When the P-CSCF on the originating side indicated support for media plane end-to-access-edge security, and the P-CSCF receives an SDP offer containing an SDES crypto attribute as defined in RFC 4568 [168], it shall examine the received SDP attributes. If the received offer contains an "a=3ge2ae:requested" SDP attribute then the P-CSCF shall act as an IMS-ALG. The P-CSCF will act as defined in 3GPP TS 23.334 [7F] as far as SDP and SRTP is concerned. In addition, the P-CSCF shall strip the "a=3ge2ae:requested" SDP attribute and the SDES crypto attribute from the received SDP offer.

When the P-CSCF on the terminating side supporting media plane end-to-access-edge security receives an SDP offer not containing SRTP as transport, it may invoke IMS-ALG procedures related to SDP and SRTP as defined in 3GPP TS 23.334 [7F] based on local policy.

NOTE 1: A possible local policy is that the IMS-ALG invokes procedures related to SDP and SRTP for Fixed-broadband IP-CAN, but not for cellular IP-CAN.

If the served UE indicated support for end-to-access-edge security, as defined in 3GPP TS 33.328 [19C], during registration and the P-CSCF indicated support for e2ae-security during registration, then upon generating an SDP offer for media plane security containing an SDES crypto attribute as defined in RFC 4568 [168], the P-CSCF shall include a SDES crypto attribute according to the profile defined in 3GPP TS 33.328 [19C] and a "a=3ge2ae:applied" SDP attribute (and other appropriate security attributes) for all media, with the following exceptions:

- a) media transported by a protocol with no supported end-to-access-edge media security mechanism; and

NOTE 2: This release of this document supports only media security mechanisms for RTP based media.

- b) media for which the result of the SDP offer / answer exchange results in the application of an end-to-end security mechanism.

### 6.7.2.3 IMS-ALG in P-CSCF for explicit congestion control support

#### 6.7.2.3.1 General

An IMS-ALG may support ECN according to RFC 6679 [188].

Subject to local policy, an IMS-ALG shall prohibit the negotiation of ECN during SDP offer/answer exchanges associated with multimedia priority service by removing any ECN attribute "a=ecn-capable-rtp" from the SDP offer and shall not invoke ECN for SIP transactions associated with multimedia priority service.

#### 6.7.2.3.2 Incoming SDP offer with ECN

If the IMS-ALG receives an SDP offer containing the "a=ecn-capable-rtp" attribute as specified in RFC 6679 [188] and:

- the IMS-ALG knows via configuration that the IMS-AGW supports transparently forwarding of ECN bits according to RFC 3168 [189];
- the IMS-ALG knows via configuration that the (IMS) network handles ECN-marked packets properly; and
- the IMS-ALG does not configure the IMS-AGW to transcode,

then the IMS-ALG shall:

- if the "ecn-capable-rtp" attribute includes both the "ice" initialisation method and other initialisation methods, remove the "ice" initialisation method from the "ecn-capable-rtp" attribute and add the attribute with this modification in the outgoing the SDP offer;

- if the "ecn-capable-rtp" attribute only includes the "ice" initialisation method, do not include the "ecn-capable-rtp" attribute in outgoing SDP offer; and
- if the "ecn-capable-rtp" attribute does not include the "ice" initialisation method include the unmodified "ecn-capable-rtp" attribute within the outgoing SDP offer.

If the IMS-ALG receives an SDP offer containing the ECN attribute "a=ecn-capable-rtp" as specified in RFC 6679 [188] and any of the following conditions apply:

- the IMS-ALG knows by configuration that the IMS-AGW does not support transparent transport of ECN-marked packets;
- the IMS-ALG knows by configuration that the (IMS) network does not properly handle ECN-marked packets; or
- the IMS-ALG does not configure the IMS-AGW to transcode,

then the IMS-ALG shall not include ECN attributes in the outgoing SDP offer, and, if the IMS-ALG knows in addition via configuration that the IMS-AGW supports acting as an ECN endpoint and that the IMS-ALG supports at least some of the initialisation methods offered within the "a=ecn-capable-rtp" attribute, the IMS-ALG shall:

- select an initialisation method supported by the IMS-AGW; and
- return a SDP answer according to the capabilities of the IMS-AGW, containing the "a=ecn-capable-rtp" attribute,

and the IMS-ALG will configure the IMS-AGW to act as an end point for ECN.

If the IMS-ALG receives an SDP answer containing the "a=ecn-capable-rtp" attribute it will instruct the IMS-AGW to transparently forward the ECN bits described in RFC 3168 [189].

### 6.7.2.3.3 Incoming SDP offer without ECN

If the IMS-ALG receives a SDP offer without the "a=ecn-capable-rtp" attribute and all of the following conditions apply:

- the IMS-ALG knows via configuration that the IMS-AGW supports acting as ECN endpoint; and
- the IMS-ALG knows via configuration that the succeeding network supports ECN,

then the IMS-ALG may include the "a=ecn-capable-rtp" attribute in the offer it forwards towards the succeeding node, indicating the related capabilities of the IMS-AGW.

If the IMS-ALG inserted ECN attributes in the SDP offer and receives an SDP answer containing the "a=ecn-capable-rtp" attribute, the IMS-ALG shall return the SDP answer to the preceding node removing the "a=ecn-capable-rtp" attribute, and will configure the IMS-AGW to act as an ECN endpoint.

### 6.7.2.4 IMS-ALG in P-CSCF for Optimal Media Routing (OMR)

Based on operator policy, the P-CSCF shall remove OMR related SDP attributes before it sends an SDP offer or answer towards an UE, as specified in subclause 2.1.9 of 3GPP TS 29.079 [11D].

### 6.7.2.5 IMS-ALG in P-CSCF for NA(P)T and NA(P)T-PT controlled by the P-CSCF

#### 6.7.2.5.1 General

This subclause describes the P-CSCF procedures for supporting the scenario where IP address and/or port conversions occur at the IMS-AGW level in the media path between the UE and the backbone. Two types of address conversions are covered:

- IP version interworking (NA(P)T-PT); and
- IP address/port translation (NA(P)T).

When the P-CSCF performs procedures for P-CSCF controlled NA(P)T and NA(P)T-PT, it shall modify the IP address(es) and port numbers (in case of NA(P)T) in SDP offers and answers, based on the IP address(es) and port number(s) received from the IMS-AGW, as described in subclause 6.7.2.1.



## 6.7.2.6 IMS-ALG in P-CSCF for support of hosted NAT

### 6.7.2.6.1 General

When the P-CSCF performs procedures for hosted NAT, it shall modify the IP address(es) and port numbers, based on the IP address(es) and number(s) received from the IMS-AGW, as described in subclause 6.7.2.1.

## 6.7.2.7 IMS-ALG in P-CSCF for support of ICE

### 6.7.2.7.1 General

This subclause describes procedures of a P-CSCF to support ICE, as defined in RFC 5245 [99].

NOTE 1: If no IMS-AGW is inserted on the media plane, a P-CSCF might transparently pass ICE related SDP attributes, in order to support ICE between the UE and remote entities. The remaining procedures in this subclause apply to when the P-CSCF inserts an IMS-ALG on the media plane.

When the P-CSCF with attached IMS-AGW receives SDP candidate information from the offerer, it shall not forward the candidate information towards the answerer. When the P-CSCF receives SDP candidate information from the answerer, it shall not forward the candidate information towards the offerer. The remaining procedures in subclause 6.7.2.7.1 are optional.

NOTE 2: An P-CSCF that removes and/or does not provide ICE related SDP attributes (e.g. a=candidate) in the offer/answer exchange will cause the ICE procedures to be aborted and the address and port information in the m and c lines of the SDP offer will be used. If this address and port information contains the relayed candidate address of a STUN Relay server, as recommended by ICE, then an extra media relay server will be used for the session which is not necessary nor desirable.

The P-CSCF with attached IMS-ALG performs separate ICE procedures towards the offerer and the answerer. The usage of ICE is negotiated separately with the offerer and answerer, and ICE may be applied independently at either side. Furthermore, the P-CSCF may be configured to apply ICE procedures only towards one network side, e.g. towards the IM CN subsystem it belongs to.

NOTE 3: Since the P-CSCF is inserting an IMS-ALG, it can choose to provide the NAT traversal mechanism defined in Annex F towards the UE. In such case the P-CSCF will not provide ICE support towards the UE, but the P-CSCF can still provide ICE support towards the core network in scenarios where ICE is used in the core network, e.g. to support NAT traversal for other access networks with no deployed IMS-ALGs.

Since the P-CSCF is not located behind a NAT, it does not request the IMS-ALG to generate keep-alive messages even when acting as a full ICE entity. The P-CSCF only requests the IMS-ALG to terminate and generate STUN messages used for the candidate selection procedures.

Since the P-CSCF is not located behind a NAT the P-CSCF shall only include host candidates in SDP offers and answers generated by the P-CSCF.

### 6.7.2.7.2 P-CSCF full ICE procedures for UDP based streams

#### 6.7.2.7.2.1 General

This subclause describes the P-CSCF full ICE procedures for UDP based streams.

#### 6.7.2.7.2.2 P-CSCF receiving SDP offer

When the P-CSCF receives an SDP offer including ICE candidate information, the P-CSCF shall send the candidate information for each UDP based stream received in the SDP offer towards the IMS-ALG. The P-CSCF shall request the IMS-ALG to reserve media- and STUN resources towards the offerer, based on the candidate information, in order to allow the IMS-ALG to perform the necessary connectivity checks per the ICE procedures.

If the offerer is acting as an ICE controller entity the P-CSCF shall act as an ICE controlled entity in the direction towards the offerer. If the offerer is acting as an ICE controlled entity the P-CSCF shall act as an ICE controller entity in the direction towards the offerer.

#### 6.7.2.7.2.3 P-CSCF sending SDP offer

Prior to sending an SDP offer, the P-CSCF may choose to apply related ICE procedures, e.g. if it expects to interact with terminals applying procedures as described in subclause K.5.2, and if both the P-CSCF and IMS-ALG also support ICE procedures. To invoking these ICE procedures, the P-CSCF shall request the IMS-ALG to reserve media- and STUN resources towards the answerer for each UDP based media stream and include a host candidate attribute for each UDP based stream in the SDP offer, providing the reserved address and port at the IMS-ALG as destination.

The P-CSCF shall always act as an ICE controller entity towards the answerer.

NOTE: The host candidate address included by the P-CSCF in the generated SDP offer matches the c- and m line information for the associated UDP stream in the SDP offer.

#### 6.7.2.7.2.4 P-CSCF receiving SDP answer

When the P-CSCF receives an SDP answer including ICE candidate information, the P-CSCF shall send the candidate information for each UDP based stream received in the SDP answer towards the IMS-ALG.

The P-CSCF shall request the IMS-ALG to perform ICE candidate selection procedures towards the answerer. The P-CSCF shall request the IMS-ALG to inform the P-CSCF, for each UDP stream, which candidate pair has been selected towards the answerer, once the candidate selection procedure towards the answerer has finished.

If the IMS-ALG indicates to the P-CSCF that, for at least one UDP stream, the selected candidate pair does not match the c- and m- line address information for the associated UDP stream, exchanged between the P-CSCF and the answerer, and the P-CSCF acts an ICE controller entity towards the answerer, the P-CSCF shall send a new offer towards the answerer in order to align the c- and m- lines address information with the chosen candidate pair for the associated UDP stream.

#### 6.7.2.7.2.5 P-CSCF sending SDP answer

When the P-CSCF generates an SDP answer for an offer that included ICE candidate information, the P-CSCF shall request the IMS-ALG to reserve media- and STUN resources towards the offerer for each UDP based media stream and include an SDP host candidate attribute for each UDP based stream in the SDP answer, providing the reserved address and port at the IMS-ALG as destination.

The P-CSCF shall in the generated SDP answer include host candidate information which matches the c- and m line information for the associated UDP stream in the SDP answer.

The P-CSCF shall request the IMS-ALG to perform ICE candidate selection procedures towards the offerer. The P-CSCF shall request the IMS-ALG to inform the P-CSCF, for each UDP stream, which candidate pair has been selected towards the offerer, once the candidate selection procedure towards the answerer has finished.

If the IMS-ALG indicates to the P-CSCF that the selected candidate pair towards the offerer does not match the c- and m- line address information for the associated UDP stream, exchanged between the P-CSCF and the offerer, and the P-CSCF acts an ICE controller entity towards the offerer, the P-CSCF shall send an offer towards the offerer (which will now act as an answerer) in order to align the c- and m- line address information with the chosen candidate pair for the associated UDP stream.

#### 6.7.2.7.3 P-CSCF ICE lite procedures for UDP based streams

When the P-CSCF is using ICE lite procedures for UDP based streams, the P-CSCF procedures are identical as described in subclause 6.7.2.7.2, with the following exceptions:

- The P-CSCF always acts as an ICE controlled entity towards the offerer and towards the answerer; and
- The P-CSCF requests the IMS-ALG to perform ICE lite candidate selection procedures, as defined in RFC 5245 [99].

#### 6.7.2.7.4 ICE procedures for TCP based streams

##### 6.7.2.7.4.1 General

The P-CSCF shall terminate ICE procedures for TCP based streams. Instead the P-CSCF will use the mechanism defined in RFC 4145 [83] for establishing TCP based streams, as defined in RFC 6544 [131].

An entity that supports ICE continues the ICE procedures for UDP based streams, even if no candidates are provided for TCP based streams.

NOTE: The P-CSCF ICE procedures for TCP based streams are identical no matter whether the P-CSCF uses full ICE or ICE lite procedures for UDP based streams.

#### 6.7.2.7.4.2 P-CSCF receiving SDP offer

When the P-CSCF receives an SDP offer, the P-CSCF shall ignore the candidate attributes for TCP based streams. The P-CSCF shall not send the candidate information for TCP based streams towards the IMS-ALG.

#### 6.7.2.7.4.3 P-CSCF sending SDP offer

When the P-CSCF generates an SDP offer the P-CSCF shall include an "actpass" setup attribute, as defined in RFC 4145 [83], for each TCP based stream, which will cause the answerer to initiate the TCP connections towards the IMS-ALG. The P-CSCF shall not include any candidate attributes for TCP based streams in the SDP offer.

#### 6.7.2.7.4.4 P-CSCF receiving SDP answer

Since the P-CSCF does not include candidates in the SDP offer towards the answerer, there are no ICE specific procedures when the P-CSCF receives an SDP answer.

NOTE: If the SDP answer contains candidate attributes for TCP based streams, the P-CSCF simply discards the candidate attributes.

#### 6.7.2.7.4.5 P-CSCF sending SDP answer

When the P-CSCF generates an SDP answer the P-CSCF shall include a "passive" setup attribute, as defined in RFC 4145 [83], for each TCP based stream, which will cause the offerer to initiate the TCP connections towards the IMS-ALG. The P-CSCF shall not include any candidate attributes for TCP based streams in the SDP answer.

### 6.7.2.8 IMS-ALG in P-CSCF for transcoding

An IMS-ALG may support procedures to modify SDP for transcoding purposes. The IMS-ALG shall only apply those transcoding procedures if an attached IMS-AGW supports transcoding.

Upon receipt of an SDP offer, based on local policy and SDP signalling inspection, the IMS-ALG may decide to offer transcoding.

To offer transcoding at the IMS-AGW, the IMS-ALG shall add codecs selected by local policy and supported by the IMS-AGW to the SDP offer. The IMS-ALG should add those codecs at the end of the codec list contained in the received SDP offer in order to give priority to the codecs inserted by the offerer over the codecs inserted by the IMS-ALG.

NOTE: RFC 4566 [39] recommends to list codecs in priority order, so by adding network inserted codecs to the end of the codec list will give higher priority to previous codecs that might have been inserted by the originating UE.

Upon receipt of the corresponding SDP answer, the IMS-ALG shall inspect the list of the codecs within the SDP answer and proceed as follows:

- If the list contains at least one of the codecs that was already contained in the previously received SDP offer, no transcoding at the IMS-AGW is required and the IMS-ALG will configure the IMS-AGW accordingly. The IMS-ALG shall remove from the SDP the codecs added to the original offer before forwarding the response to the offerer.
- If only the codecs inserted by the IMS-ALG are contained in the answer, the IMS-ALG will configure the IMS-AGW to transcode. The IMS-ALG shall replace the received codecs in the SDP answer with the codec it configured the IMS-AGW to use towards the SDP offerer's direction.

For an IMS-ALG acting as ATCF, the following applies in addition:

- During an originating or terminating session establishment, for media using PS transport towards the UE, the IMS-ALG (ATCF) should pass SDP offers without adding codecs to the SDP offer and pass SDP answers without modification to the contained codecs to avoid the potential need for transcoding in the IMS-AGW before the PS to CS access transfer; and

- during the PS to CS access transfer procedure, the IMS-ALG (ATCF) shall preferentially select from the SDP offer it receives from the MSC server the codec already configured on the corresponding remote leg, if available.

### 6.7.3 IMS-ALG in ISC gateway function

#### 6.7.3.1 General

When the ISC gateway function acts as an IMS-ALG, it makes procedures as for an originating UA and terminating UA. The IMS-ALG acts as a B2BUA. For the use of the IMS-ALG for specific capabilities, additional procedures are defined in subsequent subclauses.

NOTE: The internal function of the IBCF as an IMS-ALG is defined in 3GPP TS 29.162 [11A], and the capabilities are identical for the ISC gateway function.

#### 6.7.3.2 IMS-ALG in application gateway function for support of ICE

The application gateway function shall act according to the procedures defined for the IBCF in subclause 6.7.1.2.

---

## 7 Extensions within the present document

### 7.1 SIP methods defined within the present document

There are no SIP methods defined within the present document over and above those defined in the referenced IETF specifications.

### 7.2 SIP header fields defined within the present document

#### 7.2.0 General

There are no SIP header fields defined within the present document over and above those defined in the referenced IETF specifications.

7.2.1 Void

7.2.2 Void

7.2.3 Void

7.2.4 Void

7.2.5 Void

7.2.6 Void

7.2.7 Void

7.2.8 Void

7.2.9 Void

7.2.10 Void

## 7.2A Extensions to SIP header fields defined within the present document

### 7.2A.1 Extension to WWW-Authenticate header field

#### 7.2A.1.1 Introduction

This extension defines a new authentication parameter (auth-param) for the WWW-Authenticate header field used in a 401 (Unauthorized) response to the REGISTER request. For more information, see RFC 2617 [21] subclause 3.2.1.

#### 7.2A.1.2 Syntax

The syntax for for auth-param is specified in table 7.2A.1.

**Table 7.2A.1: Syntax of auth-param**

|               |                                    |
|---------------|------------------------------------|
| auth-param    | = 1#( integrity-key / cipher-key ) |
| integrity-key | = "ik" EQUAL ik-value              |
| cipher-key    | = "ck" EQUAL ck-value              |
| ik-value      | = LDQUOTE *(HEXDIG) RDQUOTE        |
| ck-value      | = LDQUOTE *(HEXDIG) RDQUOTE        |

#### 7.2A.1.3 Operation

This authentication parameter will be used in a 401 (Unauthorized) response in the WWW-Authenticate header field during UE authentication procedure as specified in subclause 5.4.1.

The S-CSCF appends the integrity-key parameter (directive) to the WWW.-Authenticate header field in a 401 (Unauthorized) response. The P-CSCF stores the integrity-key value and removes the integrity-key parameter from the header field prior to forwarding the response to the UE.

The S-CSCF appends the cipher-key parameter (directive) to the WWW-Authenticate header field in a 401 (Unauthorized) response. The P-CSCF removes the cipher-key parameter from the header field prior to forwarding the response to the UE. In the case ciphering is used, the P-CSCF stores the cipher-key value.

### 7.2A.2 Extension to Authorization header field

#### 7.2A.2.1 Introduction

This extension defines a new auth-param for the Authorization header field used in REGISTER requests. For more information, see RFC 2617 [21] subclause 3.2.2.

## 7.2A.2.2 Syntax

The syntax of auth-param for the Authorization header field is specified in table 7.2A.2.

**Table 7.2A.2: Syntax of auth-param for Authorization header field**

```
auth-param = "integrity-protected" EQUAL ("yes" / "no" / "tls-pending" / "tls-yes" / "ip-assoc-
pending" / "ip-assoc-yes") / "auth-done"
```

## 7.2A.2.3 Operation

This authentication parameter is inserted in the Authorization header field of all the REGISTER requests. The value of the "integrity-protected" header field parameter in the auth-param parameter is set as specified in subclause 5.2.2. This information is used by S-CSCF to decide whether to challenge the REGISTER request or not, as specified in subclause 5.4.1.

The values in the "integrity-protected" header field field are defined as follows:

- "yes": indicates that a REGISTER request received in the P-CSCF is protected using an IPsec security association and IMS AKA is used as authentication scheme.
- "no": indicates that a REGISTER request received in the P-CSCF is not protected using an IPsec security association and IMS AKA is used as authentication scheme, i.e. this is an initial REGISTER request with the Authorization header field not containing a challenge response.
- "tls-yes": indicates that a REGISTER request is received in the P-CSCF protected over a TLS connection and the Session ID, IP address and port for the TLS connection are already bound to a private user identity. The S-CSCF will decide whether or not to challenge such a REGISTER request based on its policy. This is used in case of SIP digest with TLS.
- "tls-pending": indicates that a REGISTER request is received in the P-CSCF protected over a TLS connection and the Session ID, IP address and port for the TLS connection are not yet bound to a private user identity. The S-CSCF shall challenge such a REGISTER request if it does not contain an Authorization header field with a challenge response or if the verification of the challenge response fails. This is used in case of SIP digest with TLS.
- "ip-assoc-yes": indicates that a REGISTER request received in the P-CSCF does map to an existing IP association in case SIP digest without TLS is used.
- "ip-assoc-pending": indicates that a REGISTER request received in the P-CSCF does not map to an existing IP association, and does contain a challenge response in case SIP digest without TLS is used.
- "auth-done": indicates that a REGISTER request is sent from an entity that is trusted and has authenticated the identities used in the REGISTER request. An example for such an entity is the MSC server enhanced for IMS centralized services. The S-CSCF shall skip authentication.

NOTE 1: In case of SIP digest with TLS is used, but the REGISTER request was not received over TLS, the P-CSCF does not include an "integrity-protected" header field parameter in the auth-param to indicate that an initial REGISTER request was not received over an existing TLS session. The S-CSCF will always challenge such a REGISTER request.

NOTE 2: In case of SIP digest without TLS is used, but the REGISTER request was not received over TLS, the P-CSCF does not include an "integrity-protected" header field parameter in the auth-param to indicate that the REGISTER request does not map to an existing IP association, and does not contain a challenge response. The S-CSCF will always challenge such a REGISTER request.

NOTE 3: The value "yes" is also used when an initial REGISTER request contains an Authorization header field with a challenge response as in this case the IPsec association is already in use, and its use by the UE implicitly authenticates the UE. This is a difference to TLS case where the use of TLS alone does not yet implicitly authenticates the UE. Hence in the TLS case, for an initial REGISTER request containing an Authorization header field with a challenge response the value "tls-pending" and not "tls-yes" is used.

## 7.2A.3 Tokenized-by header field parameter definition (various header fields)

### 7.2A.3.1 Introduction

The "tokenized-by" header field parameter is an extension parameter appended to encrypted entries in various SIP header fields as defined in subclause 5.10.4.

### 7.2A.3.2 Syntax

The syntax for the "tokenized-by" header field parameter is specified in table 7.2A.3:

**Table 7.2A.3: Syntax of tokenized-by-param**

```
rr-param = tokenized-by-param / generic-param
via-params = via-ttl / via-maddr
            / via-received / via-branch
            / tokenized-by-param / via-extension
tokenized-by-param = "tokenized-by" EQUAL hostname
```

The BNF for rr-param and via-params is taken from RFC 3261 [26] and modified accordingly.

### 7.2A.3.3 Operation

The "tokenized-by" header field parameter is appended by IBCF (THIG) after all encrypted strings within SIP header fields when network configuration hiding is active. The value of the header field parameter is the domain name of the network which encrypts the information.

## 7.2A.4 P-Access-Network-Info header field

### 7.2A.4.1 Introduction

The P-Access-Network-Info header field is extended to include specific information relating to particular access technologies.

### 7.2A.4.2 Syntax

The syntax of the P-Access-Network-Info header field is described in RFC 7315 [52] and RFC 7913 [234]. There are additional coding rules for this header field depending on the type of IP-CAN, according to access technology specific descriptions.

Table 7.2A.4 describes the 3GPP-specific extended syntax of the P-Access-Network-Info header field defined in RFC 7315 [52] and RFC 7913 [234].

**Table 7.2A.4: Syntax of extended P-Access-Network-Info header field**

```
operator-specific-GI = "operator-specific-GI" EQUAL (token / quoted-string)
utran-sai-3gpp       = "utran-sai-3gpp" EQUAL (token / quoted-string)
```

The operator-specific-GI and utran-sai-3gpp parameters are instances of generic-param from the current extension-access-info component of the P-Access-Network-Info header field defined in RFC 7315 [52] and RFC 7913 [234].

The presence of the "np" parameter defined in RFC 7315 [52] indicates a P-Access-Network-Info header field is provided by the P-CSCF, S-CSCF, the AS, the MSC server enhanced for ICS or by the MGCF. The content can differ from a P-Access-Network-Info header field without this parameter which is provided by the UE.

The "np" parameter can be used with both "access-type" and "access-class" constructs. The "access-class" construct is provided for use where the value is not known to be specific to a particular "access-type" value, e.g. in the case of some values delivered from the PCRF. The "access-class" field can be set only by the P-CSCF. The "np" parameter can be set

only by the P-CSCF, S-CSCF, the AS, the MSC server enhanced for ICS or by the MGCF. The "local-time-zone" parameter, the "gstin-location" parameter and the "GSTN" value of access-type field shall not be inserted by the UE.

The "local-time-zone" parameter defined in RFC 7315 [52] indicates the time difference between local time and UTC of day. For 3GPP accesses, the "local-time-zone" parameter represents the time zone allocated to the routing area or traffic area which the UE is currently using. As the edge of such areas may overlap, there can be some discrepancy with the actual time zone of the UE where the UE is in the near proximity to a time zone boundary.

#### 7.2A.4.3 Additional coding rules for P-Access-Network-Info header field

The P-Access-Network-Info header field is populated with the following contents:

- 1) the access-type field set to one of "3GPP-GERAN", "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP-E-UTRAN-FDD", "3GPP-E-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "3GPP2-UMB", "3GPP2-1X-Femto", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", "IEEE-802.11g", "IEEE-802.11n", "ADSL", "ADSL2", "ADSL2+", "RADSL", "SDSL", "HDSL", "HDSL2", "G.SHDSL", "VDSL", "IDSL", or "DOCSIS", "IEEE-802.3", "IEEE-802.3a", "IEEE-802.3e", "IEEE-802.3i", "IEEE-802.3j", "IEEE-802.3u", or "IEEE-802.3ab", "IEEE-802.3ae", "IEEE-802.3ah", "IEEE-802.3ak", "IEEE-802.3aq", "IEEE-802.3an", "IEEE-802.3y", "IEEE-802.3z" or "DVB-RCS2" as appropriate to the access technology in use.
- 1A) the access-class field set to one of "3GPP-GERAN", "3GPP-UTRAN", "3GPP-E-UTRAN", "3GPP-WLAN", "3GPP-GAN", "3GPP-HSPA", or "3GPP2" as appropriate to the technology in use.
- 2) if the access type field or the access-class field is set to "3GPP-GERAN", a cgi-3gpp parameter set to the Cell Global Identity obtained from lower layers of the UE. The Cell Global Identity is a concatenation of MCC, MNC, LAC and CI (as described in 3GPP TS 23.003 [3]). The value of "cgi-3gpp" parameter is therefore coded as a text string as follows:
 

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and CI (fixed length code of 16 bits using a full hexadecimal representation);
- 3) if the access type field is equal to "3GPP-UTRAN-FDD", or "3GPP-UTRAN-TDD", and a UE provides the P-Access-Network-Info header field, a "utran-cell-id-3gpp" parameter set to a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003 [3]) and the UMTS Cell Identity (as described in 3GPP TS 25.331 [9A]), obtained from lower layers of the UE, and is coded as a text string as follows:
 

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and UMTS Cell Identity (fixed length code of 28 bits using a full hexadecimal representation);
- 3A) if the access type field is equal to "3GPP-UTRAN-FDD", or "3GPP-UTRAN-TDD", and an entity that can use the "np" parameter provides the P-Access-Network-Info header field, a "utran-sai-3gpp" parameter set to a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003 [3]) and the Service Area Code (SAC) (as described in 3GPP TS 23.003 [3]), and is coded as a text string as follows:
 

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and SAC (fixed length code of 16 bits using a full hexadecimal representation).
- 3B) if the access class field is equal to "3GPP-UTRAN", or "3GPP-HSPA", a "utran-sai-3gpp" parameter set to a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003 [3]) and the Service Area Code (SAC) (as described in 3GPP TS 23.003 [3]), and is coded as a text string as follows:
 

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and SAC (fixed length code of 16 bits using a full hexadecimal representation).
- 4) void
- 5) if the access type field is set to "3GPP2-1X", a ci-3gpp2 parameter set to the ASCII representation of the hexadecimal value of the string obtained by the concatenation of SID (16 bits), NID (16 bits), PZID (8 bits) and BASE\_ID (16 bits) (see 3GPP2 C.S0005-D [85]) in the specified order. The length of the ci-3gpp2 parameter shall be 14 hexadecimal characters. The hexadecimal characters (A through F) shall be coded using the uppercase ASCII characters. If the UE does not know the values for any of the above parameters, the UE shall



use the value of 0 for that parameter. For example, if the SID is unknown, the UE shall represent the SID as 0x0000;

NOTE 1: The SID value is represented using 16 bits as supposed to 15 bits as specified in 3GPP2 C.S0005-D [85].

EXAMPLE: If SID = 0x1234, NID = 0x5678, PZID = 0x12, BASE\_ID = 0xFFFF, the ci-3gpp2 value is set to the string "1234567812FFFF".

- 6) if the access type field is set to "3GPP2-1X-HRPD", a ci-3gpp2 parameter set to the ASCII representation of the hexadecimal value of the string obtained by the concatenation of Sector ID (128 bits) and Subnet length (8 bits) (see 3GPP2 C.S0024-B [86]) and Carrier-ID, if available, (see 3GPP2 X.S0060 [86B]) in the specified order. The length of the ci-3gpp2 parameter shall be 34 or 40 hexadecimal characters depending on whether the Carrier-ID is included. The hexadecimal characters (A through F) shall be coded using the uppercase ASCII characters;

EXAMPLE: If the Sector ID = 0x12341234123412341234123412341234, Subnet length = 0x11, and the Carrier-ID=0x555444, the ci-3gpp2 value is set to the string "123412341234123412341234123411555444".

- 7) if the access type field is set to "3GPP2-UMB" 3GPP2 C.S0084-000 [86A], a ci-3gpp2 parameter is set to the ASCII representation of the hexadecimal value of the Sector ID (128 bits) defined in 3GPP2 C.S0084-000 [86A]. The length of the ci-3gpp2 parameter shall be 32 hexadecimal characters. The hexadecimal characters (A through F) shall be coded using the uppercase ASCII characters;

EXAMPLE: If the Sector ID = 0x12341234123412341234123412341234, the ci-3gpp2 value is set to the string "1234123412341234123412341234".

- 8) if the access-type field set to one of "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b" or "IEEE-802.11g", or "IEEE-802.11n", an "i-wlan-node-id" parameter is set to the ASCII representation of the hexadecimal value of the AP's MAC address without any delimiting characters;

EXAMPLE: If the AP's MAC address = 00-0C-F1-12-60-28, then i-wlan-node-id is set to the string "000cf1126028".

- 9) if the access type field is set to "3GPP2-1X-Femto", a ci-3gpp2-femto parameter set to the ASCII representation of the hexadecimal value of the string obtained by the concatenation of femto MSCID (24 bit), femto CellID (16 bit), FEID (64bit), macro MSCID (24 bits) and macro CellID (16 bits) (3GPP2 X.P0059-200 [86E]) in the specified order. The length of the ci-3gpp2-femto parameter is 36 hexadecimal characters. The hexadecimal characters (A through F) are coded using the uppercase ASCII characters.

- 10) if the access-type field is set to one of "ADSL", "ADSL2", "ADSL2+", "RADSL", "SDSL", "HDSL", "HDSL2", "G.SHDSL", "VDSL", "IDSL", the access-info field shall contain a dsl-location parameter obtained from the CLF (see NASS functional architecture);

- 11) if the access-type field set to "DOCSIS", the access info parameter is not inserted. This release of this specification does not define values for use in this parameter;

- 12) if the access type field is equal to "3GPP-E-UTRAN-FDD" or "3GPP-E-UTRAN-TDD", a "utran-cell-id-3gpp" parameter set to a concatenation of the MCC, MNC, Tracking Area Code as described in 3GPP TS 23.003 [3] and the E-UTRAN Cell Identity (ECI) as described in 3GPP TS 23.003 [3], and is coded as a text string as follows:

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), Tracking Area Code (fixed length code of 16 bits using full hexadecimal representation) and ECI (fixed length code of 28 bits using a full hexadecimal representation);

- 12A) if the access class field is equal to "3GPP-E-UTRAN", a "utran-cell-id-3gpp" parameter set to a concatenation of the MCC, MNC, Tracking Area Code as described in 3GPP TS 23.003 [3] and the E-UTRAN Cell Identity (ECI) as described in 3GPP TS 23.003 [3], and is coded as a text string as follows:

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), Tracking Area Code (fixed length code of 16 bits using full hexadecimal representation) and ECI (fixed length code of 28 bits using a full hexadecimal representation);

- 13) if the access-type field is set to one of "IEEE-802.3", "IEEE-802.3a", "IEEE-802.3e", "IEEE-802.3i", "IEEE-802.3j", "IEEE-802.3u", "IEEE-802.3ab", "IEEE-802.3ae", "IEEE-802.3ak", "IEEE-802.3aq", "IEEE-802.3an",

"IEEE-802.3y" or "IEEE-802.3z" and NASS subsystem is used, the access-info field shall contain an eth-location parameter obtained from the CLF (see NASS functional architecture);

14) if the access-type field is set to one of "GPON", "XGPON1" or "IEEE-802.3ah" and NASS is used, the access-info field shall contain an fiber-location parameter obtained from the CLF (see NASS functional architecture);

15) if the access-type field is set to "GSTN", the access-info field may contain a gstn-location parameter if received from the GSTN; and

NOTE 2: The "cgi-3gpp", the "utran-cell-id-3gpp", the "ci-3gpp2", the "ci-3gpp2-femto", the "i-wlan-node-id", eth-location, and the "dsl-location" parameters described above among other usage also constitute the location identifiers that are used for emergency services.

16) if the access-type field is set to "DVB-RCS2", the access-info field shall contain a "dvb-rcs2-node-id" parameter which consists of comma-separated list consisting of NCC\_ID, satellite\_ID, beam\_ID, and SVN-MAC as specified in ETSI TS 101 545-2 [194], ETSI TS 101 545-3 [195]; the NCC\_ID shall be represented as two digit hexadecimal value, the satellite\_ID shall be represented as a two digit hexadecimal value, the beam\_ID shall be represented as a four digit hexadecimal value, and the SVN-MAC shall be represented as six digit hexadecimal value.

EXAMPLE: If the (8 bit) NCC\_ID = 0x3A, the (8 bit) satellite\_ID = 0xF5, the (16 bit) beam\_ID = 0xEA23, and the (24 bit) SVN-MAC = 0xE40AB9, then the "dvb-rcs2-node-id" is set to the string "3A,F5,EA23,E40AB9".

17) the local-time-zone-parameter in access-info field is coded as a text string as follows:

UTC±[hh]:[mm]. [hh] is two digits from 00 to 13, and [mm] is two digits from four values: "00", "15", "30" or "45", see ISO 8601 [203].

EXAMPLE: "UTC+01:00" indicates that the time difference between local time and UTC of day is one hour.

20) the operator-specific-GI in an access-info field is coded as text string and conveys an operator-specific geographical identifier.

## 7.2A.5 P-Charging-Vector header field

### 7.2A.5.1 Introduction

The P-Charging-Vector header field is extended to include specific charging correlation information needed for IM CN subsystem functional entities.

### 7.2A.5.2 Syntax

#### 7.2A.5.2.1 General

The syntax of the P-Charging-Vector header field is described in RFC 7315 [52]. There may be additional coding rules for this header field depending on the type of IP-CAN, according to access technology specific descriptions.

Table 7.2A.5 describes 3GPP-specific extensions to the P-Charging-Vector header field defined in RFC 7315 [52].

Table 7.2A.5: Syntax of extensions to P-Charging-Vector header field

```

access-network-charging-info = (gprs-charging-info / i-wlan-charging-info / xdsl-charging-info /
    packetcable-charging-info / icn-charging-info / eps-charging-info / eth-charging-info /
    loopback-indication / generic-param)
gprs-charging-info = ggsn SEMI auth-token [SEMI pdp-info-hierarchy] *(SEMI extension-param)
ggsn = "ggsn" EQUAL gen-value
pdp-info-hierarchy = "pdp-info" EQUAL LDQUOT pdp-info *(COMMA pdp-info) RDQUOT
pdp-info = pdp-item SEMI pdp-sig SEMI gcid [SEMI flow-id]
pdp-item = "pdp-item" EQUAL DIGIT
pdp-sig = "pdp-sig" EQUAL ("yes" / "no")
gcid = "gcid" EQUAL 1*HEXDIG
auth-token = "auth-token" EQUAL 1*HEXDIG
flow-id = "flow-id" EQUAL "(" "{" 1*DIGIT COMMA 1*DIGIT "}" *(COMMA "{" 1*DIGIT COMMA 1*DIGIT
    "}")")"
extension-param = token [EQUAL token]
i-wlan-charging-info = "pdg"
xdsl-charging-info = bras SEMI auth-token [SEMI xDSL-bearer-info] *(SEMI extension-param)
bras = "bras" EQUAL gen-value
xDSL-bearer-info = "dsl-bearer-info" EQUAL LDQUOT dsl-bearer-info *(COMMA dsl-bearer-info) RDQUOT
dsl-bearer-info = dsl-bearer-item SEMI dsl-bearer-sig SEMI dslcid [SEMI flow-id]
dsl-bearer-item = "dsl-bearer-item" EQUAL DIGIT
dsl-bearer-sig = "dsl-bearer-sig" EQUAL ("yes" / "no")
dslcid = "dslcid" EQUAL 1*HEXDIG
packetcable-charging-info = packetcable [SEMI bcid]
packetcable = "packetcable-multimedia"
bcid = "bcid" EQUAL 1*48(HEXDIG)
icn-charging-info = icn-bcp *(SEMI itid) [SEMI extension-param]
icn-bcp = "icn-bcp" EQUAL gen-value
itid = itc-sig SEMI itc-id SEMI *(flow-id)
itc-sig = "itc-sig" EQUAL ("yes" / "no")
itc-id = "itc-id" EQUAL gen-value
flow-id = "flow-id" EQUAL gen-value
extension-param = token [EQUAL (token | quoted-string)]
eps-charging-info = pdngw [SEMI eps-bearer-hierarchy] *(SEMI extension-param)
pdngw = "pdngw" EQUAL gen-value
eps-bearer-hierarchy = "eps-info" EQUAL LDQUOT eps-info *(COMMA eps-info) RDQUOT
eps-info = eps-item SEMI eps-sig SEMI ecid [SEMI flow-id]
eps-item = "eps-item" EQUAL DIGIT
eps-sig = "eps-sig" EQUAL ("yes" / "no")
ecid = "ecid" EQUAL 1*HEXDIG
eth-charging-info = ip-edge *(SEMI extension-param)
fiber-charging-info = ip-edge *(SEMI extension-param)
ip-edge = "ip-edge" EQUAL gen-value
extension-param = token [EQUAL (token | quoted-string)]
loopback-indication = "loopback"

```

**NOTE:** The syntax above is not aligned with the rules for defining new P-Charging-Vector header field parameters as defined in RFC 3455 [52]. Entities that perform syntax check (even if they are not interested in specific header field parameter values) of the header field need to follow the explicit syntax above, as using the rules in RFC 3455 [52] would trigger a parser error.

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header field.

The access-network-charging-info parameter includes alternative definitions for different types access networks. The description of these parameters are given in the subsequent subclauses.

The "access-network-charging-info" header field parameter is not included in the P-Charging-Vector for SIP signalling that is not associated with a session.

When the "access-network-charging-info" is included in the P-Charging-Vector and necessary information is not available from the IP-CAN (e.g. via Gx/Rx interface) reference points then null or zero values are included.

For type 1 and type 3 IOIs, the generating SIP entity shall express the "orig-ioi" and "term-ioi" header field parameters in the format of a quoted string as specified in RFC 7315 [52] with a specific string prefix being "Type 1" and "Type 3" respectively to indicate the type of IOI. For the type 2 IOI, no string prefix is used. The receiving SIP entity does not perform syntactic checking of the contents of the IOI parameter (the IOI parameter is passed unmodified to charging entities).

The "loopback" parameter is provided to the charging system of other entities in the signalling path to indicate that loopback has been applied and entities of the IM CN subsystem involved in the loopback, e.g TRF, will have generated CDRs in their own right.

#### 7.2A.5.2.2 GPRS as IP-CAN

GPRS is a supported access network (gprs-charging-info parameter). For GPRS there are the following components to track: GGSN address (ggsn parameter), media authorization token (auth token parameter), and a pdp-info parameter that contains the information for one or more PDP contexts. In this release the media authorization token is set to zero. The pdp-info contains one or more pdp-item values followed by a collection of parameters (pdp-sig, gcid, and flow-id). The value of the pdp-item is a unique number that identifies each of the PDP-related charging information within the P-Charging-Vector header field. Each PDP context has an indicator if it is an IM CN subsystem signalling PDP context (pdp-sig parameter), an associated GPRS Charging Identifier (gcid parameter), and a identifier (flow-id parameter). The flow-id parameter contains a sequence of curly bracket delimited flow identifier tuples that identify associated m-lines and relative order of port numbers in an m-line within the SDP from the SIP signalling to which the PDP context charging information applies. For a complete description of the semantics of the flow-id parameter see 3GPP TS 29.214 [13D] Annex B. The gcid, ggsn address and flow-id parameters are transferred from the GGSN to the P-CSCF via the PCRF over the Rx interface (see 3GPP TS 29.214 [13D] and Gx interface (see 3GPP TS 29.212 [13B]).

The gcid value is received in binary format at the P-CSCF (see 3GPP TS 29.214 [13D]). The P-CSCF shall encode it in hexadecimal format before include it into the gcid parameter. On receipt of this header field, a node receiving a gcid shall decode from hexadecimal into binary format.

The "access-network-charging-info" is not included in the P-Charging-Vector for SIP signalling that is not associated with a multimedia session. The access network charging information may be unavailable for sessions that use a general purpose PDP context (for both SIP signalling and media) or that do not require media authorisation.

#### 7.2A.5.2.3 I-WLAN as IP-CAN

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header field.

This version of the specification defines the use of "pdg" for inclusion in the P-Charging-Vector header field. No other extensions are defined for use in I-WLAN in this version of the specification.

#### 7.2A.5.2.4 xDSL as IP-CAN

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header field. The access-network-charging-info parameter includes alternative definitions for different types of access networks. This subclause defines the components of the xDSL instance of the access-network-charging-info.

For xDSL, there are the following components to track: BRAS address (bras parameter), media authorization token (auth-token parameter), and a set of dsl-bearer-info parameters that contains the information for one or more xDSL bearers.

The dsl-bearer-info contains one or more dsl-bearer-item values followed by a collection of parameters (dsl-bearer-sig, dslcid, and flow-id). The value of the dsl-bearer-item is a unique number that identifies each of the dsl-bearer-related charging information within the P-Charging-Vector header field. Each dsl-bearer-info has an indicator if it is an IM CN subsystem signalling dsl-bearer (dsl-bearer-sig parameter), an associated DSL Charging Identifier (dslcid parameter), and a identifier (flow-id parameter). The flow-id parameter contains a sequence of curly bracket delimited flow identifier tuples that identify associated m-lines and relative order of port numbers in an m-line within the SDP from the SIP signalling to which the dsl-bearer charging information applies. For a complete description of the semantics of the flow-id parameter see 3GPP TS 29.214 [13D].

The format of the dslcid parameter is identical to that of ggsn parameter. On receipt of this header field, a node receiving a dslcid shall decode from hexadecimal into binary format.

For a dedicated dsl-bearer for SIP signalling, i.e. no media stream requested for a session, then there is no authorisation activity or information exchange over the Rx and Gx interfaces. Since there are no dslcid, media authorization token or flow identifiers in this case, the dslcid and media authorization token are set to zero and no flow identifier parameters are constructed by the PCRF.

#### 7.2A.5.2.5 DOCSIS as IP-CAN

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header field. The access-network-charging-info parameter includes alternative definitions for different types of access networks. This subclause defines the components of the cable instance of the access-network-charging-info. Cable access is based upon the architecture defined by Data Over Cable Service Interface Specification (DOCSIS).

The billing correlation identifier (bcid) uniquely identifies the PacketCable DOCSIS bearer resources associated with the session within the cable operator's network for the purposes of billing correlation. To facilitate the correlation of session and bearer accounting events, a correlation ID that uniquely identifies the resources associated with a session is needed. This is accomplished through the use of the bcid as generated by the PacketCable Multimedia network. This bcid is returned to the P-CSCF within the response to a successful resource request.

The bcid is specified in RFC 3603 [74A]. This identifier is chosen to be globally unique within the system for a window of several months. Consistent with RFC 3603 [74A], the BCID must be encoded as a hexadecimal string of up to 48 characters. Leading zeroes may be suppressed.

If the bcid value is received in binary format by the P-CSCF from the IP-CAN, the P-CSCF shall encode it in hexadecimal format before including it into the bcid parameter. On receipt of this header field, a node using a bcid will normally decode from hexadecimal into binary format.

#### 7.2A.5.2.6 cdma2000<sup>®</sup> packet data subsystem as IP-CAN

The specific extensions to the P-Charging-Vector header field defined in RFC 7315 [52] when the access network is cdma2000<sup>®</sup> packet data subsystem are: the icn-charging-info parameter contains one icn-bcp child parameter and one or more child itid parameters. The icn-bcp parameter, identifies the point of attachment where UE has attached itself to the cdma2000<sup>®</sup> packet data subsystem. The icn-bcp parameter is conveyed to the P-CSCF by the cdma2000<sup>®</sup> packet data subsystem. Each itid child parameter within icn-charging-info corresponds to one IP-CAN bearer that was established by the cdma2000<sup>®</sup> packet data subsystem for the UE. Each itid parameter contains an indicator if it is an IP-CAN subsystem signalling IP-CAN bearer (itc-sig parameter), an associated IP-CAN charging identifier (itc-id parameter), and one or more flow identifiers (flow-id parameter) that identify associated m-lines within the SDP from the SIP signalling. These parameters are transferred from the cdma2000<sup>®</sup> packet data subsystem to the P-CSCF over the respective interface.

For an IP-CAN bearer that is only used for SIP signalling, i.e. no media stream requested for a session, then there is no authorisation activity or information exchange with the P-CSCF over the respective cdma2000<sup>®</sup> interfaces. Since there is no itc-id, or flow identifiers in this case, the itc-id is set to zero and no flow identifier parameters are constructed by the P-CSCF.

#### 7.2A.5.2.7 EPS as IP-CAN

For EPS there are the following components to track: P-GW address (pdngw parameter), and a eps-info parameter that contains the information for one or more EPS bearers. The eps-info contains one or more eps-item values followed by a collection of parameters (eps-sig, ecid, and flow-id). The value of the eps-item is a unique number that identifies each of the EPS-bearer-related charging information within the P-Charging-Vector header field. Each EPS bearer context has an associated QCI indicating if it is an IM CN subsystem signalling EPs bearer context (eps-sig parameter), an associated EPS Charging Identifier (ecid parameter), and a identifier (flow-id parameter). The flow-id parameter contains a sequence of curly bracket delimited flow identifier tuples that identify associated m-lines and relative order of port numbers in an m-line within the SDP from the SIP signalling to which the EPS bearer charging information applies. For a complete description of the semantics of the flow-id parameter see 3GPP TS 29.214 [13D] Annex B. The ecid, pdngw address and flow-id parameters are transferred from the P-GW to the P-CSCF via the PCRF over the Rx interface (see 3GPP TS 29.214 [13D] and Gx interface (see 3GPP TS 29.212 [13B]).

The ecid value is received in binary format at the P-CSCF (see 3GPP TS 29.214 [13D]). The P-CSCF shall encode it in hexadecimal format before include it into the ecid parameter. On receipt of this header field, a node receiving a gcid shall decode from hexadecimal into binary format.

The "access-network-charging-info" header field parameter is not included in the P-Charging-Vector for SIP signalling that is not associated with a multimedia session. The access network charging information may be unavailable for sessions that use a general purpose EPS bearer context (for both SIP signalling and media).

### 7.2A.5.2.8 Ethernet as IP-CAN

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header field. For Ethernet accesses, the IP Edge Node address (ip-edge parameter) is tracked. The IP Edge Node is defined in ETSI ES 282 001 [138].

### 7.2A.5.2.9 Fiber as IP-CAN

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header field. For Fiber accesses, the IP Edge Node address (ip-edge parameter) is tracked. The IP Edge Node is defined in ETSI ES 282 001 [138].

### 7.2A.5.3 Operation

The operation of this header field is described in subclauses 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8.

## 7.2A.6 Orig parameter definition

### 7.2A.6.1 Introduction

The "orig" parameter is a uri-parameter intended to:

- tell the S-CSCF that it has to perform the originating services instead of terminating services;
- tell the I-CSCF that it has to perform originating procedures.

### 7.2A.6.2 Syntax

The syntax for the orig parameter is specified in table 7.2A.6:

**Table 7.2A.6: Syntax of orig parameter**

```
uri-parameter = transport-param / user-param / method-param / ttl-param / maddr-param / lr-param /
               orig / other-param
orig = "orig"
```

The BNF for uri-parameter is taken from RFC 3261 [26] and modified accordingly.

### 7.2A.6.3 Operation

The orig parameter is appended to the address of the S-CSCF, I-CSCF or IBCF by the ASs, when those initiate requests on behalf of the user, or to the address of the S-CSCF or I-CSCF by an IBCF acting as entry point, if the network is performing originating service to another network. The S-CSCF will run originating services whenever the orig parameter is present next to its address. The I-CSCF will run originating procedures whenever the orig parameter is present next to its address. The IBCF will preserve the "orig" parameter in the topmost Route header field if received, or it may append the "orig" parameter to the URI in the topmost Route header field (see subclause 5.10.2.3).

## 7.2A.7 Extension to Security-Client, Security-Server and Security-Verify header fields

### 7.2A.7.1 Introduction

This extension defines new parameters for the Security-Client, Security-Server and Security-Verify header fields.

This subclause defines the "mediasec" header field parameter that labels any of the Security-Client:, Security-Server, or Security-Verify: header fields as applicable to the media plane and not the signalling plane.

## 7.2A.7.2 Syntax

### 7.2A.7.2.1 General

The syntax for the Security-Client, Security-Server and Security-Verify header fields is defined in RFC 3329 [48]. The additional syntax is defined in Annex H of 3GPP TS 33.203 [19].

This specification reuses Security-Client, Security-Server and Security-Verify defined in RFC 3329 [48] and defines the mechanisms listed in table 7.2A.7.2.2-2 and the header field parameter "mediasec".

Security mechanisms that apply to the media plane only shall not have the same name as any signalling plane mechanism. If a signalling plane security mechanism name is re-used for the media plane and distinguished only by the "mediasec" parameter, then implementations that do not recognize the "mediasec" parameter may incorrectly use that security mechanism for the signalling plane.

### 7.2A.7.2.2 "mediasec" header field parameter

The "mediasec" header field parameter may be used in the Security-Client, Security-Server, or Security-Verify header fields defined in RFC 3329 [48] to indicate that a header field applies to the media plane. Any one of the media plane security mechanisms supported by both client and server, if any, may be applied when a media stream is started. Or, a media stream may be set up without security.

Values in the Security-Client, Security-Server, or Security-Verify header fields labelled with the "mediasec" header field parameter are specific to the media plane and specific to the secure media transport protocol used on the media plane.

EXAMPLE: Security-Client: sdes-srtp;mediasec

Usage of the "mediasec" header field parameter in mech-parameters rule of RFC 3329 [48] and the syntax of mediasec header field parameter is shown in table 7.2A.7.2.2-1.

**Table 7.2A.7.2.2-1**

```
mech-parameters = / mediasec-param
mediasec-param = "mediasec"
```

The security mechanisms which can be labelled by the "mediasec" header field parameter are listed in the table 7.2A.7.2.2-2, where each line (other than the first line) indicates a token and a media security mechanism for which the token indicates support.

**Table 7.2A.7.2.2-2**

```
mechanism-name/ = ( sdes-srtp-name / token )
sdes-srtp-name = "sdes-srtp" ; End-to-access-edge media security using SDES.
```

## 7.2A.7.3 Operation

The operation of the additional parameters for the Security-Client, Security-Server and Security-Verify header fields is defined in Annex H of 3GPP TS 33.203 [19].

Any one of the mechanisms listed in table 7.2A.7.2.2-2 and labelled with the "mediasec" header field parameter can be applied on-the-fly as a media stream is started, unlike mechanisms for signalling one of which is chosen and then applied throughout a session.

Media plane security can be supported independently of any signalling plane security defined in RFC 3329 [4], but in order to protect any cryptographic key carried in SDP signalling plane security as defined in RFC 3329 [4] SHOULD be used.

The message flow is identical to the flow in RFC 3329 [48], but it is not mandatory for the user agent to apply media plane security immediately after it receives the list of supported media plane mechanisms from the server, or any timer after that, nor will the lack of a mutually supported media plane security mechanism prevent SIP session setup.

## 7.2A.7.4 IANA registration

### 7.2A.7.4.1 "mediasec" header field parameter

**Editor's note:** [MEDIASEC\_CORE, CR 4156] This subclause forms the basis for IANA registration of the mediasec header field parameter. Registration is intended to be created by an RFC that describes the mediasec header field parameter and creates an IANA registry for its values.

**NOTE:** This subclause contains information to be provided to IANA for the registration of the media plane security indicator header field parameter.

Contact name, email address, and telephone number:

3GPP Specifications Manager

3gppContact@etsi.org

+33 (0)492944200

Header field in which the parameter can appear:

Security-Client, Security-Server and Security-Verify header fields.

Name of the header field parameter being registered:

mediasec

Whether the parameter only accepts a set of predefined values:

No value is defined for the parameter.

A reference to the RFC where the parameter is defined and to any RFC that defines new values for the parameter:

This parameter is defined in 3GPP TS 24.229.

### 7.2A.7.4.2 "sdes-srtp" security mechanism

**Editor's note:** [MEDIASEC\_CORE, CR 4156] This subclause forms the basis for IANA registration of the value for the mediasec header field parameter. The registration should be performed by MCC when the registry for mediasec parameter values has been created by IANA.

**NOTE:** This subclause contains information to be provided to IANA for the registration of the media plane security indicator header field parameter.

Contact name, email address, and telephone number:

3GPP Specifications Manager

3gppContact@etsi.org

+33 (0)492944200

The mechanism-name token

Mechanism name (as it will appear in SIP)

sdes-srtp

The published RFC describing the details of the corresponding security mechanism:

This mechanism is defined in 3GPP TS 24.229.



## 7.2A.8 IMS Communication Service Identifier (ICSI)

### 7.2A.8.1 Introduction

The ICSI is defined to fulfil the requirements as stated in 3GPP TS 23.228 [7]. An ICSI may have specialisations which refine it by adding subclass identifiers separated by dots. Any specialisations of an ICSI shall have an "is a" relationship if the subclasses are removed. For example, a check for ICSI urn:urn-7:3gpp-service.ims.icsi.mmtel will return true when evaluating ICSI urn:urn-7:3gpp-service.ims.icsi.mmtel.hd-video.

### 7.2A.8.2 Coding of the ICSI

This parameter is coded as a URN. The ICSI URN may be included as:

- a tag-value within the g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62], in which case those characters of the URN that are not part of the tag-value definition in RFC 3840 [62] shall be represented in the percent encoding as defined in RFC 3986 [124];
- a feature cap value within the "g.3gpp.icsi-ref" feature-capability indicator, as defined in subclause 7.9A.1 and RFC 6809 [190], in which case those characters of the URN that are not part of the feature-capability indicator value definition syntax shall be represented in the percent encoding, as defined in RFC 3986 [124]; or
- as a value of the P-Preferred-Service or P-Asserted-Service header fields as defined RFC 6050 [121].

A list of the URNs containing ICSI values registered by 3GPP can be found at <http://www.3gpp.com/Uniform-Resource-Name-URN-list.html>

An example of an ICSI for a 3GPP defined IMS communication service is:

```
urn:urn-7:3gpp-service.ims.icsi.mmtel
```

An example of a g.3gpp.icsi-ref media feature tag containing an ICSI for a 3GPP defined IMS communication service is:

```
g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
```

An example of a g.3gpp.icsi-ref feature-capability indicator containing an ICSI for a 3GPP defined IMS communication service is:

```
g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"
```

An example of an ICSI for a 3GPP defined IMS communication service in a P-Preferred-Service header field is

```
P-Preferred-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel
```

An example of an ICSI for a 3GPP defined IMS communication service in a P-Asserted-Service header field is

```
P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel
```

An example of an ICSI for a defined IMS communication service with a specialisation is:

```
P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel.game-v1
```

An example of an ICSI for a 3GPP defined IMS communication service with an organisation-y defined specialisation is:

```
P-Asserted-Service: urn:urn-7:3gpp-service.ims.icsi.mmtel.organisation-y.game-v2
```

## 7.2A.9 IMS Application Reference Identifier (IARI)

### 7.2A.9.1 Introduction

The IARI is defined to fulfil the requirements as stated in 3GPP TS 23.228 [7].

### 7.2A.9.2 Coding of the IARI

This parameter is coded as a URN. The IARI URN may be included as a tag-value within the g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62], in which case those characters of the URN that are not part of the tag-value definition in RFC 3840 [62] shall be represented in the percent encoding as defined in RFC 3986 [124].

A list of the URNs containing IARI values registered by 3GPP can be found at <http://www.3gpp.com/Uniform-Resource-Name-URN-list.html>

An example of a g.3gpp.iari-ref media feature tag containing an IARI is:

```
g.3gpp.iari-ref="urn%3Aurn-7%3A3gpp-application.ims.iari.game-v1"
```

## 7.2A.10 "phone-context" tel URI parameter

### 7.2A.10.1 Introduction

The "phone-context" tel URI parameter indicates that the UE uses local service number or that the UE has included information according to a local dialling plan in the Request-URI.

In the former case, the "phone-context" tel URI parameter is included in a Tel-URI or a corresponding SIP URI with a "user" SIP URI parameter set to "phone".

In the latter case, the "phone-context" tel URI parameter is included in the user part of a SIP URI with the "user" SIP URI parameter set to "dialstring" (see RFC 4967 [103]).

### 7.2A.10.2 Syntax

The syntax of the "phone-context" tel URI parameter is described in RFC 3966 [22]. There are additional coding rules for this parameter depending on the type of IP-CAN, according to access technology specific descriptions.

### 7.2A.10.3 Additional coding rules for "phone-context" tel URI parameter

In case the current IP-CAN is indicated in the "phone-context" tel URI parameter, the entities inserting the "phone-context" tel URI parameter shall populate the "phone-context" tel URI parameter with the following contents:

- 1) if the IP-CAN is GPRS, then the "phone-context" tel URI parameter is a domain name. It is constructed from the MCC, the MNC and the home network domain name by concatenating the MCC, MNC, and the string "gprs" as domain labels before the home network domain name;

EXAMPLE: If MCC = 216, MNC = 01, then the "phone-context" tel URI parameter is set to '216.01.gprs.home1.net'.

- 2) if the IP-CAN is I-WLAN, then the "phone-context" tel URI parameter is a domain name. It is constructed from the SSID, AP's MAC address, and the home network domain name by concatenating the SSID, AP's MAC address, and the string "i-wlan" as domain labels before the home network domain name;

EXAMPLE: If SSID = BU-Airport, AP's MAC = 00-0C-F1-12-60-28, and home network domain name is "home1.net", then the "phone-context" tel URI parameter is set to the string "bu-airport.000cf1126028.i-wlan.home1.net".

- 3) if the IP-CAN is xDSL, then the "phone-context" tel URI parameter is a domain name. It is constructed from the dsl-location (see subclause 7.2A.4) and the home network domain name by concatenating the dsl-location and the string "xdsl" as domain labels before the home network domain name;
- 4) if the IP-CAN is DOCSIS, then the "phone-context" tel URI parameter is based on data configured locally in the UE;
- 5) if the IP-CAN is EPS, then the "phone-context" tel URI parameter is a domain name. It is constructed from the MCC, the MNC and the home network domain name by concatenating the MCC, MNC, and the string "eps" as domain labels before the home network domain name;
- 6) if the IP-CAN is Ethernet, then the "phone-context" parameter is a domain name. It is constructed from the eth-location (see subclause 7.2A.4) and the home network domain name by concatenating the eth-location and the string "ethernet" as domain labels before the home network domain name;
- 7) if the IP-CAN is Fiber, then the "phone-context" parameter is a domain name. It is constructed from the fiber-location (see subclause 7.2A.4) and the home network domain name by concatenating the fiber-location and the string "fiber" as domain labels before the home network domain name;

- 8) if the IP-CAN is cdma2000®, then the "phone-context" parameter is a domain name. It is constructed from the subnet id and the home network domain name by concatenating the subnet id as the domain label before the home network domain name;
- 9) if the IP-CAN is DVB-RCS2, then the "phone-context" tel URI parameter is based on data configured locally in the UE; and
- 10) if the access network information is not available in the UE, then the "phone-context" tel URI parameter is set to the home network domain name preceded by the string "geo-local."

In case the home domain is indicated in the "phone-context" tel URI parameter, the "phone-context" tel URI parameter is set to the home network domain name (as it is used to address the SIP REGISTER request, see subclause 5.1.1.1A or subclause 5.1.1.1B).

In case the "phone-context" tel URI parameter indicates a network other than the home network or the visited access network, the "phone-context" tel URI parameter is set according to RFC 3966 [22].

## 7.2A.11 Void

7.2A.11.1 Void

7.2A.11.2 Void

7.2A.11.3 Void

## 7.2A.12 CPC and OLI tel URI parameter definition

### 7.2A.12.1 Introduction

The use of the "cpc" and "oli" URI parameters for use in the P-Asserted-Identity in SIP requests is defined.

### 7.2A.12.2 Syntax

The Calling Party's Category and Originating Line Information are represented as URI parameters for the tel URI scheme and SIP URI representation of telephone numbers. The ABNF syntax is as follows and extends the formal syntax for the tel URI as specified in RFC 3966 [22]:

**Table 7.2A.7**

```

par = / cpc / oli
cpc = cpc-tag "=" cpc-value
oli = oli-tag "=" oli-value
cpc-tag = "cpc"
oli-tag = "oli"
cpc-value
= "ordinary" / "test" / "operator" /
"payphone" / "unknown" / "mobile-hplmn" / "mobile-vplmn" / "emergency" /
genvalue
oli-value = 2DIGIT
genvalue = 1*(alphanum / "-" / ".")

```

The Accept-Language header field shall be used to express the language of the operator.

The semantics of these Calling Party's Category values are described below:

**ordinary:** The caller has been identified, and has no special features.

**test:** This is a test call that has been originated as part of a maintenance procedure.

**operator:** The call was generated by an operator position.

**payphone:** The calling station is a payphone.

**unknown:** The CPC could not be ascertained.

**mobile-hplmn:** The call was generated by a mobile device in its home PLMN.

**mobile-vplmn:** The call was generated by a mobile device in a visited PLMN.

**emergency:** The call is an emergency service call.

NOTE 1: The choice of CPC and OLI values and their use are up to the Service Provider. CPC and OLI values can be exchanged across networks if specified in a bilateral agreement between the service providers.

NOTE 2: Additional national/regional CPC values can exist.

The two digit OLI values are decimal codes assigned and administered by North American Numbering Plan Administration.

### 7.2A.12.3 Operation

The "cpc" and "oli" URI parameters may be supported by IM CN subsystem entities that provide the UA role and by IM CN subsystem entities that provide the proxy role.

The "cpc" and "oli" URI parameters shall not be populated at the originating UE.

Unless otherwise specified in this document, "cpc" and "oli" URI parameters are only passed on by IM CN subsystem entities (subject to trust domain considerations as specified in subclause 4.4.12).

## 7.2A.13 "sos" SIP URI parameter

### 7.2A.13.1 Introduction

The "sos" SIP URI parameter is intended to:

- indicate to the S-CSCF that a REGISTER request that includes the "sos" SIP URI parameter is for emergency registration purposes;
- tell the S-CSCF to not apply barring of the public user identity being registered; and
- tell the S-CSCF to not apply initial filter criteria to requests destined for an emergency registered contact.

### 7.2A.13.2 Syntax

The syntax for the "sos" SIP URI parameter is specified in table 7.8

**Table 7.2A.8: Syntax of sos SIP URI parameter**

|  |
|--|
| <pre>uri-parameter = / sos-param sos-param = "sos"</pre> |
|--|

The BNF for uri-parameter is taken from RFC 3261 [26] and modified accordingly.

### 7.2A.13.3 Operation

When a UE includes the "sos" SIP URI parameter in the URI included in the Contact header field of REGISTER request, the REGISTER request is intended for emergency registration.

When a S-CSCF receives a REGISTER request for emergency registration that includes the "sos" SIP URI parameter, the S-CSCF is required to preserve the previously registered contact address. This differs to the registrar operation as defined in RFC 3261 [26] in that the rules for URI comparison for the Contact header field shall not apply and thus, if the URI in the Contact header field matches a previously received URI, then the old contact address shall not be overwritten.

## 7.2A.14 P-Associated-URI header field

Procedures of RFC 7315 [52] are modified to allow a SIP proxy to remove URIs from the P-Associated-URI header field.

## 7.2A.15 Void

## 7.2A.16 Extension to History-Info header field

### 7.2A.16.1 Introduction

This extension defines a new hi-target-param (mp-param) for the History-Info header field. The mp-param indicates the Targeted-to-URI is another user mapped from Request-URI in the incoming request that was retargeted.

### 7.2A.16.2 Syntax

The syntax of the History-Info header field is described in RFC 4244 [66]. The additional syntax for "mp-param" is specified in table 7.2A.16.

**Table 7.2A.16: Syntax of "mp-param"**

```

hi-param = hi-target-param
hi-target-param = mp-param
mp-param = "mp" EQUAL index-val
index-val = number *("." number)
number = [ %x31-39 *DIGIT ] DIGIT

```

### 7.2A.16.3 Operation

The "mp" header field parameter indicates that the hi-targeted-to-URI represents a user other than the target user associated with the Request-URI in the incoming request that was retargeted. This occurs when a request is statically or dynamically retargeted to another user represented by an AOR unassociated with the AOR of the original target user. The "mp" header field parameter contains the value of the hi-index in the hi-entry with a hi-targeted-to-uri that reflects the Request-URI that was retargeted, thus identifying the "mapped from" target.

If the service the AS provides needs to deliver the original destination identity to the UE, the AS shall either:

- 1) if the History-Info header field is present in the incoming request, insert a new hi-entry to the History-Info header field, including an "mp" header field parameter; or
- 2) if the History-Info header field is not present in the incoming request:
  - a) insert a History-Info header field with the first hi-entry including the received Request-URI; and
  - b) insert the second hi-entry including the target URI with an "mp" header field parameter containing the value of hi-index in the first entry.

## 7.3 Option-tags defined within the present document

There are no option-tags defined within the present document over and above those defined in the referenced IETF specifications.

## 7.4 Status-codes defined within the present document

There are no status-codes defined within the present document over and above those defined in the referenced IETF specifications.

## 7.5 Session description types defined within the present document

### 7.5.1 General

This subclause contains definitions for SDP parameters that are specific to SDP usage in the 3GPP IM CN Subsystem and therefore are not described in an RFC.

## 7.5.2 End-to-access-edge media plane security

### 7.5.2.1 General

The end-to-access-edge security-indicator is used to indicate that a UE requests a P-CSCF to apply media plane security or to indicate that a P-CSCF has applied end-to-access-edge security as defined in 3GPP TS 33.328 [19C].

### 7.5.2.2 Syntax

3GPP end-to-access-edge security indicator is a value attribute which is encoded as a media-level SDP attribute with the ABNF syntax defined in table 7.5.1. ABNF is defined in RFC 2234 [20G].

**Table 7.5.1: ABNF syntax of 3ge2ae attribute**

```
3ge2ae-attribute = "a=3ge2ae:" indicator
indicator = "requested" / "applied" / token
```

"requested": the sender indicates its wish that end-to-access-edge security is applied.

"applied": the sender indicates that it has applied end-to-access-edge security.

This version of the specification only defines usage of the "requested" and "applied" attribute values. Other values shall be ignored.

The "3ge2ae" attribute is charset-independent.

### 7.5.2.3 IANA registration

**NOTE:** This subclause contains information to be provided to IANA for the registration of the end-to-access-edge security indicator SDP attribute.

Contact name, email address, and telephone number:

3GPP Specifications Manager

3gppContact@etsi.org

+33 (0)492944200

Attribute Name (as it will appear in SDP)

3ge2ae

Long-form Attribute Name in English:

3GPP\_e2ae-security-indicator

Type of Attribute

Media level

Is Attribute Value subject to the Charset Attribute?

This Attribute is not dependent on charset.

Purpose of the attribute:

This attribute specifies the end-to-access-edge security-indicator as used for IMS media plane security

Appropriate Attribute Values for this Attribute:

The attribute is a value attribute. The values "requested" and "applied" are defined.

## 7.5.3 Optimal Media Routeing (OMR) attributes

### 7.5.3.1 General

The SDP attributes associated with OMR are used to identify and select alternative media plane paths for the purpose of bypassing unneeded media functions in the network, as described in 3GPP TS 29.079 [11D].

### 7.5.3.2 Semantics

The visited-realm attribute contains an IP realm identifier and transport address for a media function in the media plane that can potentially be used to bypass other allocated media functions.

The secondary-realm attribute contains an IP realm identifier and transport address for an alternate media function in the media plane that can potentially be used to bypass other allocated media functions.

The `omr-s-cksum` and `omr-m-cksum` attributes includes checksums for session level information and media level information to identify if the SDP was altered by intermediaries in such a way as to invalidate OMR information present in the SDP.

The `"omr-codecs"`, `"omr-m-att"` and `"omr-s-att"` attributes contain codec-related SDP offer information encapsulated by a SIP-ALG in the signalling path that has modified codec related information.

The `"omr-m-bw"` and `"omr-s-bw"` attributes contain bandwidth-related SDP offer information encapsulated by a SIP-ALG in the signalling path that has modified codec related information.

Each group of zero or more versions of each of the `"omr-codecs"`, `"omr-m-att"`, `"omr-s-att"`, `"omr-m-bw"` and `"omr-s-bw"` attributes for a media line with the same instance number is associated with the visited-realm instance for the modified media line and represents the version of the SDP information for the media line before modifications.

### 7.5.3.3 Syntax

The syntax specified in table 7.5.2 uses the augmented Backus-Naur Form as described in RFC 2234 [20G].

Table 7.5.2: Syntax OMR attributes

|   |  |   |
|---|--|---|
| visited-realm                           | = "visited-realm" ":" instance-number SP                 |   |
| realm SP                                |  |   |
| nettype SP                              |  | ;from RFC 4566 [39]   |
| addrtype SP                             |  | ;from RFC 4566 [39]   |
| connection-address SP                   |  | ;from RFC 4566 [39]   |
| port                                    |  | ;from RFC 4566 [39]   |
| [SP rtcp-port [SP rtcp-address]]        |  |   |
| *(SP extension-name SP extension-value) |  |   |
| secondary-realm                         | = "secondary-realm" ":" instance-number SP               |   |
| realm SP                                |  |   |
| nettype SP                              |  | ;from RFC 4566 [39]   |
| addrtype SP                             |  | ;from RFC 4566 [39]   |
| connection-address SP                   |  | ;from RFC 4566 [39]   |
| port                                    |  | ;from RFC 4566 [39]   |
| [SP rtcp-port [SP rtcp-address]]        |  |   |
| *(SP extension-name SP extension-value) |  |   |
| instance-number                         | = 1*DIGIT  |   |
| realm                                   | = non-ws-string  | ;from RFC 4566 [39]   |
| rtcp-port                               | = "rtcp-port" SP port                                    |   |
| rtcp-address                            | = "rtcp-address" SP connection-address                   |   |
| extension-name                          | = token  | ;shall be different to existing tokens "previsous-fmt", "rtcp-port" and "rtcp-address". |
| extension-value                         | = non-ws-string  |   |
| omr-m-cksum                             | = "omr-m-cksum" ":" 1*HEXDIG                             |   |
| omr-s-cksum                             | = "omr-s-cksum" ":" 1*HEXDIG                             |   |
| omr-codecs                              | = "omr-codecs" ":" instance-number SP proto 1*(SP fmt)   | ;from RFC 4566 [39]   |
| omr-m-att                               | = "omr-m-att" ":" instance-number SP attribute           | ;from RFC 4566 [39]   |
| omr-s-att                               | = "omr-s-att" ":" instance-number SP attribute           | ;from RFC 4566 [39]   |
| omr-m-bw                                | = "omr-m-bw" ":" instance-number SP bwtype ":" bandwidth | ;from RFC 4566 [39]   |
| omr-s-bw                                | = "omr-s-bw" ":" instance-number SP bwtype ":" bandwidth | ;from RFC 4566 [39]   |

This grammar encodes the primary media level information about each visited-realm and secondary-realm instance: the sequence in which the realm was visited, the realm identity, its IP address and port:

<instance-number>: instance-number is a positive decimal integer which identifies the sequence in which this visited-realm was added during the forwarding of an SDP offer. If an IMS-ALG adds second-realm attribute(s), omr-codecs attribute(s), omr-m-att attribute(s), omr-s-att attribute(s), omr-m-bw attribute(s) and/or the omr-s-bw attribute(s) to an SDP offer it will assign the same instance number as assigned to the visited-realm attribute for the forwarded SDP offer. When used in the SDP answer, the instance-number, realm, nettype and addrtype uniquely identify the corresponding visited-realm or secondary-realm instance from the SDP offer.

<realm>: identifies a set of mutually reachable IP endpoints that share a common IP addressing scheme.

Effective application of OMR depends on the scope of each realm being determined by reachability and not by administrative domain. A public IPv4 or IPv6 address reachable from the open internet shall be associated with the special realm "IN". For application to OMR in IPv6 networks, a realm corresponds to an IPv6 autonomous system.

Entity operators must adhere to the following guidelines for creation of an OMR realm string to ensure the integrity of the visited-realm and secondary-realm instance information for their realm(s): 1) Realm strings must be globally unique. It is recommended that a realm string contain a hostname or domain name, following the recommendation in subclause 3.2.1 of RFC 2617 [21], 2) Realm strings should present a human-readable identifier that can be rendered to a user.



<nettype>, <addrtype> and <connection-address>: are taken from the connection-field (c= line) of RFC 4566 [39]. They describe the IP address associated with the visited-realm or secondary-realm instance, allowing for IPv4 addresses, IPv6 addresses and FQDNs. The connection-address can be either an IP address or an FQDN.

<port>: It is the port associated with the visited-realm or secondary-realm instance as taken from RFC 4566 [39]. Its meaning depends on the network being used for the connection-address, and on the transport protocol selected for the corresponding media line, e.g., UDP or TCP.

<rtcp-port> and <rtcp-address>: taken together are semantically equivalent to the rtcp attribute defined in RFC 3605 [37A]. They optionally encode the RTCP port and address information when the RTCP port number is not exactly one greater than the port for an RTP stream at the same address.

The previous-fmt-list may be supplied within the visited-realm if this attribute is included in an SDP offer and shall not be supplied if this attribute is included in an SDP answer.

The visited-realm and secondary-realm attributes can be extended via <extension-name> and <extension-value>. The grammar allows for new name/value pairs to be added at the end of the attribute.

<omr-m-cksum>: is a hex value calculated on the contents of the media level information per media line.

<omr-s-cksum>: is a hex value calculated on the contents of the session level information.

<omr-codecs> provides the transport format <proto> and list of media formats (e.g., payload type numbers) <fmt> supported by the visited-realm instance immediately preceding the instance identified by <instance-number>. Transport format <proto> and media format <fmt> are defined in RFC 4566 [39] for the SDP m-line.

<omr-m-att> provides a media level SDP attribute <attribute> supported by the visited-realm instance immediately preceding the instance identified by <instance-number>. Attribute <attribute> is defined in RFC 4566 [39] for the SDP a-line.

<omr-s-att> provides a session level SDP attribute <attribute> supported by the visited-realm instance immediately preceding the instance identified by <instance-number>. Attribute <attribute> is defined in RFC 4566 [39] for the SDP a-line.

<omr-m-bw> provides a media level SDP bandwidth described by <bwtype> and <bandwidth> supported by the visited-realm instance immediately preceding the instance identified by <instance-number>. <bwtype> and <bandwidth> are defined in RFC 4566 [39] for the SDP b-line.

<omr-s-bw> provides a session level SDP bandwidth described by <bwtype> and <bandwidth> supported by the visited-realm instance immediately preceding the instance identified by <instance-number>. <bwtype> and <bandwidth> are defined in RFC 4566 [39] for the SDP b-line.

The "visited-realm", "secondary-realm", "omr-m-cksum", "omr-s-cksum", "omr-codecs", "omr-m-att", "omr-s-att" "omr-m-bw" and "omr-s-bw" SDP attributes are media-level attributes.

### 7.5.3.4 IANA registration

#### 7.5.3.4.1 visited-realm attribute

Contact Name: 3GPP Specifications Manager, [3gppContact@etsi.org](mailto:3gppContact@etsi.org), +33 (0)492944200

Attribute Name: visited-realm

Long Form: visited-realm

Type of Attribute: media level

Charset Considerations: The attribute is not subject to the charset attribute.

Purpose: This attribute is used in networks employing OMR procedures allowing to bypass border gateways in configurations in which IP realms are re-entered when establishing an end-to-end multimedia session. This attribute is used to identify configurations in which IP realms are re-entered when establishing an end-to-end multimedia session, so that border gateways can be bypassed without compromising their role in securing access to the networks. The attribute provides a means to identify connection information for visited IP realms to help select the most optimal available path.

Appropriate Values: See table 7.5.2.

#### 7.5.3.4.2 secondary-realm attribute

Contact Name: 3GPP Specifications Manager, [3gppContact@etsi.org](mailto:3gppContact@etsi.org), +33 (0)492944200

Attribute Name: secondary-realm

Long Form: secondary-realm

Type of Attribute: media level

Charset Considerations: The attribute is not subject to the charset attribute.

Purpose: This attribute is used in networks employing OMR procedures allowing to bypass border gateways in configurations in which IP realms are re-entered when establishing an end-to-end multimedia session. This attribute is used to identify configurations in which secondary IP realms are available to establish an end-to-end multimedia session, so that border gateways can be bypassed without compromising their role in securing access to the networks. The attribute provides a means to identify connection information for secondary IP realms to help select the most optimal available path.

Appropriate Values: See table 7.5.2.

#### 7.5.3.4.3 omr-s-cksum attribute

Contact Name: 3GPP Specifications Manager, [3gppContact@etsi.org](mailto:3gppContact@etsi.org), +33 (0)492944200

Attribute Name: omr-s-cksum

Long Form: omr-s-cksum

Type of Attribute: media level

Charset Considerations: The attribute is not subject to the charset attribute.

Purpose: This attribute is used in networks employing OMR procedures allowing to bypass border gateways in configurations in which IP realms are re-entered when establishing an end-to-end multimedia session. This attribute is used to provide a means to verify that session level SDP information has not been modified by intermediate SIP nodes not supporting the OMR procedures. The attribute provides a checksum calculated value against the session level information. Any OMR information associated with unexpectedly modified media information will be discarded.

Appropriate Values: See table 7.5.2.

#### 7.5.3.4.4 omr-m-cksum attribute

Contact Name: 3GPP Specifications Manager, [3gppContact@etsi.org](mailto:3gppContact@etsi.org), +33 (0)492944200

Attribute Name: omr-m-cksum

Long Form: omr-m-cksum

Type of Attribute: media level

Charset Considerations: The attribute is not subject to the charset attribute.

Purpose: This attribute is used in networks employing OMR procedures allowing to bypass border gateways in configurations in which IP realms are re-entered when establishing an end-to-end multimedia session. This attribute is used to provide a means to verify that media level SDP information has not been modified by intermediate SIP nodes not supporting the OMR procedures. The attribute provides a checksum calculated value against the media level information associated with the media stream for which the checksum is provided. Any OMR information associated with unexpectedly modified media information will be discarded.

Appropriate Values: See table 7.5.2.

#### 7.5.3.4.5 omr-codecs attribute

Contact Name: 3GPP Specifications Manager, [3gppContact@etsi.org](mailto:3gppContact@etsi.org), +33 (0)492944200

Attribute Name: omr-codecs

Long Form: omr-codecs

Type of Attribute: media level

Charset Considerations: The attribute is not subject to the charset attribute.

Purpose: This attribute is used in networks employing OMR procedures allowing to bypass border gateways in configurations in which IP realms are re-entered when establishing an end-to-end multimedia session. The attribute provides a means to encapsulate codec related SDP information transport format and list of media formats that are applicable if a particular border gateway is bypassed.

Appropriate Values: See table 7.5.2.

#### 7.5.3.4.6 omr-m-att attribute

Contact Name: 3GPP Specifications Manager, [3gppContact@etsi.org](mailto:3gppContact@etsi.org), +33 (0)492944200

Attribute Name: omr-m-att

Long Form: omr-m-att

Type of Attribute: media level

Charset Considerations: The attribute is not subject to the charset attribute.

Purpose: This attribute is used in networks employing OMR procedures allowing to bypass border gateways in configurations in which IP realms are re-entered when establishing an end-to-end multimedia session. The attribute provides means to encapsulate a media-level SDP attribute that is applicable if a particular border gateway is bypassed.

Appropriate Values: See table 7.5.2.

#### 7.5.3.4.7 omr-s-att attribute

Contact Name: 3GPP Specifications Manager, [3gppContact@etsi.org](mailto:3gppContact@etsi.org), +33 (0)492944200

Attribute Name: omr-s-att

Long Form: omr-s-att

Type of Attribute: media level

Charset Considerations: The attribute is not subject to the charset attribute.

Purpose: This attribute is used in networks employing OMR procedures allowing to bypass border gateways in configurations in which IP realms are re-entered when establishing an end-to-end multimedia session. The attribute provides means to encapsulate a session-level SDP attribute that is applicable if a particular border gateway is bypassed.

Appropriate Values: See table 7.5.2.

#### 7.5.3.4.8 omr-m-bw attribute

Contact Name: 3GPP Specifications Manager, [3gppContact@etsi.org](mailto:3gppContact@etsi.org), +33 (0)492944200

Attribute Name: omr-m-bw

Long Form: omr-m-bw

Type of Attribute: media level

Charset Considerations: The attribute is not subject to the charset attribute.

Purpose: This attribute is used in networks employing OMR procedures allowing to bypass border gateways in configurations in which IP realms are re-entered when establishing an end-to-end multimedia session. The attribute provides means to encapsulate a media-level SDP bandwidth that is applicable if a particular border gateway is bypassed.

Appropriate Values: See table 7.5.2.

#### 7.5.3.4.9 omr-s-bw attribute

Contact Name: 3GPP Specifications Manager, [3gppContact@etsi.org](mailto:3gppContact@etsi.org), +33 (0)492944200

Attribute Name: omr-s-bw

Long Form: omr-s-bw

Type of Attribute: media level

Charset Considerations: The attribute is not subject to the charset attribute.

Purpose: This attribute is used in networks employing OMR procedures allowing to bypass border gateways in configurations in which IP realms are re-entered when establishing an end-to-end multimedia session. The attribute provides means to encapsulate a session-level SDP bandwidth that is applicable if a particular border gateway is bypassed.

Appropriate Values: See table 7.5.2.

## 7.6 3GPP IM CN subsystem XML body

### 7.6.1 General

This subclause contains the 3GPP IM CN Subsystem XML body in XML format. The 3GPP IM CN Subsystem XML shall be valid against the 3GPP IM CN Subsystem XML schema defined in table 7.6.1.

Any SIP User Agent or proxy may insert or remove the 3GPP IM CN subsystem XML body or parts of it, as required, in any SIP message. The 3GPP IM CN subsystem XML body shall not be forwarded outside a 3GPP network.

See subclause 7.6.4 and subclause 7.6.5 for the associated MIME type definition.

### 7.6.2 Document Type Definition

The XML Schema, is defined in table 7.6.1.

**Table 7.7.6.1: IM CN subsystem XML body, XML Schema**

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
  attributeFormDefault="unqualified" version="1">
  <xs:complexType name="tIMS3GPP">
    <xs:sequence>
      <xs:choice>
        <xs:element name="alternative-service" type="tAlternativeService"/>
        <xs:element name="service-info" type="xs:string"/>
      </xs:choice>
      <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="version" type="xs:decimal" use="required"/>
    <xs:anyAttribute/>
  </xs:complexType>
  <xs:complexType name="tAlternativeService">
    <xs:sequence>
      <xs:element ref="type"/>
      <xs:element name="reason" type="xs:string"/>
      <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:anyAttribute/>
  </xs:complexType>

  <!-- root element -->
  <xs:element name="ims-3gpp" type="tIMS3GPP"/>

  <xs:element name="type" type="xs:string"/>

  <!-- action element for //ims-3gpp//alternative-service -->
  <xs:element name="action" type="xs:string"/>
</xs:schema>

```

### 7.6.3 XML Schema description

This subclause describes the elements of the IM CN subsystem XML Schema as defined in table 7.6.1.

- <ims-3gpp>**: The **<ims-3gpp>** element is the root element of the IM CN subsystem XML body. It is always present. XML instance documents of future versions of the XML Schema in table 7.6.1 is valid against the XML Schema in table 7.6.1 in this document. XML instance documents of the XML Schema in table 7.6.1 in the present document have a version attribute value, part of the **<ims-3gpp>** element, that is equal to the value of the XML Schema version described in the present document.
- <service-info>**: the transparent element received from the HSS for a particular trigger point are placed within this optional element.
- <alternative-service>**: in the present document, the alternative service is used as a response for an attempt to establish an emergency session within the IM CN subsystem or as a response to initiate S-CSCF restoration procedures. The element describes an alternative service where the call should success. The alternative service is described by the type of service information. A possible reason cause why an alternative service is suggested may be included.

In the present document, the **<alternative-service>** element contains a **<type>** element, a **<reason>** element, and an optional **<action>** element.

The **<type>** element indicates the type of alternative service. The **<type>** element contains only the values specified in table 7.6.2 in the present document.

**Table 7.6.2: ABNF syntax of values of the <type> element**

```

emergency-value = %x65.6D.65.72.67.65.6E.63.79 ; "emergency"
restoration-value = %x72.65.73.74.6F.72.61.74.69.6F.6E ; "restoration"

```

The **<action>** element contains only the values specified in table 7.6.3 in the present document.

**Table 7.6.3: ABNF syntax of values of the <action> element**

```

emergency-registration-value = %x65.6D.65.72.67.65.6E.63.79.2D.72.65.67.69.73.74.72.61.74.69.6F.6E ;
"emergency-registration"
initial-registration-value = %x69.6E.69.74.69.61.6C.2D.72.65.67.69.73.74.72.61.74.69.6F.6E ;
"initial-registration"

```

The <reason> element contains an explanatory text with the reason why the session setup has been redirected. A UE may use this information to give an indication to the user.

If included in the IM CN subsystem XML body:

1. the <type> element with the value "emergency" is included as the first child element of the <alternative-service> element;
2. the <type> element with the value "restoration" is included as one of the following:
  - a) the first child element of the <alternative-service> element; or
  - b) the third or later child element of the <alternative-service> element;
3. the <action> element with the value "emergency-registration" is included as the third child element of the <alternative-service> element; and
4. the <action> element with value "initial-registration" is included as the third or later child element of the <alternative-service> element.

NOTE: When included, the <action> and the second occurrence of the <type> elements are validated by the <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> particle of their parent elements.

## 7.6.4 MIME type definition

### 7.6.4.1 Introduction

This subclause defines the MIME type for "application/3gpp-ims+xml". A 3GPP IM CN subsystem XML Document can be identified with this media type.

### 7.6.4.2 Syntax

The following optional parameters are defined:

- "charset": the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in RFC 3023 [132].
- "sv" or "schemaversion": the syntax for the "sv" or "schemaversion" parameter is specified in table 7.6.4:

**Table 7.6.4: Syntax of the "sv" or "schemaversion" parameter**

```

m-parameter      =/ ("sv" / "schemaversion") EQUAL LDQUOTE [ sv-value-list ] RDQUOTE
sv-value-list    = sv-value-range *( "," sv-value )
sv-value-range  = sv-value [ "-" sv-value ]
sv-value         = number / token
number          = 1*DIGIT [ "." 1*DIGIT ]

```

The BNF for m-parameter is taken from RFC 3261 [26] and modified accordingly.

### 7.6.4.3 Operation

The encoding considerations for "application/3gpp-ims+xml" are identical to those of "application/xml" as described in RFC 3023 [132].

The "sv" or "schemaversion" parameter's value is used to indicate:

- the versions of the 3GPP IM CN Subsystem XML schema that can be used to validate the 3GPP IM CN subsystem XML body (if the MIME type and parameter are present in the Content-Type header field); or
- the accepted versions of the 3GPP IM CN Subsystem XML body (if the MIME type and parameter are present in the Accept header field).

If the "sv" and "schemaversion" parameter are absent, it shall be assumed that version 1 of the XML Schema for the IM CN subsystem XML body is supported.

## 7.6.5 IANA Registration

NOTE: RFC 4288 [xy], subclause 9, states the process that applies in case of changes to the registry of media types. Any future changes to the format or to subclause 7.6.5 would invoke this procedure.

MIME media type name:

application

MIME subtype name:

3gpp-ims+xml

Required parameters:

None

Optional parameters:

"charset" the parameter has identical semantics to the charset parameter of the "application/xml" media type as specified in RFC 3023 [132].

"sv" or "schemaversion" the parameter's value is used to indicate:

- the versions of the 3GPP IP Multimedia (IM) Core Network (CN) subsystem XML schema that can be used to validate the 3GPP IM CN subsystem XML body (if the MIME type and parameter are present in the Content-Type header field); or
- the accepted versions of the 3GPP IM CN Subsystem XML body (if the MIME type and parameter are present in the Accept header field).

If the "sv" and "schemaversion" parameter are absent, it shall be assumed that version 1 of the XML Schema for the IM CN subsystem XML body is supported.

Encoding considerations:

Same as encoding considerations of application/xml as specified in RFC 3023 [132]

Security considerations:

Same as general security considerations for application/xml as specified in subclause 10 of RFC 3023 [132].

In addition, this content type provides a format for exchanging information in SIP, so the security considerations from RFC 3261 [26] apply.

Interoperability considerations:

Same as Interoperability considerations as specified in subclause 3.1 of RFC 3023 [132].

If both "sv" and "schemaversion" are specified, then the value of "schemaversion" is ignored

Published specification:

3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), stage 3", as published in subclause 7.6.5, version 8.9.0.

Available via <<http://www.3gpp.org/specs/numbering.htm>>.

Applications which use this media:

Applications that use the 3GPP IM CN Subsystem as defined by 3GPP.

Intended usage:

COMMON

Additional information:

1. Magic number(s): none
2. File extension(s): none
3. Macintosh file type code: none
4. Object Identifiers: none

## 7.7 SIP timers

The timers defined in RFC 3261 [26] need modification in some cases to accommodate the delays introduced by the air interface processing and transmission delays. Table 7.7.1 shows recommended values for IM CN subsystem.

Table 7.7.1 lists in the first column, titled "SIP Timer" the timer names as defined in RFC 3261 [26].

The second column, titled "value to be applied between IM CN subsystem elements" lists the values recommended for network elements e.g. P-CSCF, S-CSCF, MGCF, when communicating with each other i.e. when no air interface leg is included. These values are identical to those recommended by RFC 3261 [26].

The third column, titled "value to be applied at the UE" lists the values recommended for the UE, when in normal operation the UE generates requests or responses containing a P-Access-Network-Info header field which included a value of "3GPP-GERAN", "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP-E-UTRAN-FDD", "3GPP-E-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "3GPP2-UMB", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", "IEEE-802.11g", "IEEE-802.11n", or "DVB-RCS2". These are modified when compared to RFC 3261 [26] to accommodate the air interface delays. In all other cases, the UE should use the values specified in RFC 3261 [26] as indicated in the second column of table 7.7.1.

The fourth column, titled "value to be applied at the P-CSCF toward a UE" lists the values recommended for the P-CSCF when an air interface leg is traversed, and which are used on all SIP transactions on a specific security association where the security association was established using a REGISTER request containing a P-Access-Network-Info header field provided by the UE which included a value of "3GPP-GERAN", "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP-E-UTRAN-FDD", "3GPP-E-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "3GPP2-UMB", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", "IEEE-802.11g", "IEEE-802.11n", or "DVB-RCS2". These are modified when compared to RFC 3261 [26]. In all other cases, the P-CSCF should use the values specified in RFC 3261 [26] as indicated in the second column of table 7.7.1.

The final column reflects the timer meaning as defined in RFC 3261 [26].



Table 7.7.1: SIP timers

| SIP Timer | Value to be applied between IM CN subsystem elements   | Value to be applied at the UE    | Value to be applied at the P-CSCF toward a UE | Meaning  |
|-----------|--|----------------------------------|---|--|
| T1        | 500ms default (see NOTE)   | 2s default                       | 2s default                                    | RTT estimate   |
| T2        | 4s (see NOTE)  | 16s                              | 16s   | The maximum retransmit interval for non-INVITE requests and INVITE responses |
| T4        | 5s (see NOTE)  | 17s                              | 17s   | Maximum duration a message will remain in the network                        |
| Timer A   | initially T1   | initially T1                     | initially T1                                  | INVITE request retransmit interval, for UDP only                             |
| Timer B   | 64*T1  | 64*T1                            | 64*T1   | INVITE transaction timeout timer   |
| Timer C   | > 3min   | > 3 min                          | > 3 min                                       | proxy INVITE transaction timeout   |
| Timer D   | > 32s for UDP<br>0s for TCP/SCTP   | >128s<br>0s for TCP/SCTP         | >128s<br>0s for TCP/SCTP                      | Wait time for response retransmits   |
| Timer E   | initially T1   | initially T1                     | initially T1                                  | non-INVITE request retransmit interval, UDP only                             |
| Timer F   | 64*T1  | 64*T1                            | 64*T1   | non-INVITE transaction timeout timer   |
| Timer G   | initially T1   | initially T1                     | initially T1                                  | INVITE response retransmit interval  |
| Timer H   | 64*T1  | 64*T1                            | 64*T1   | Wait time for ACK receipt.   |
| Timer I   | T4 for UDP<br>0s for TCP/SCTP  | T4 for UDP<br>0s for TCP/SCTP    | T4 for UDP<br>0s for TCP/SCTP                 | Wait time for ACK retransmits  |
| Timer J   | 64*T1 for UDP<br>0s for TCP/SCTP   | 64*T1 for UDP<br>0s for TCP/SCTP | 64*T1 for UDP<br>0s for TCP/SCTP              | Wait time for non-INVITE request retransmits                                 |
| Timer K   | T4 for UDP<br>0s for TCP/SCTP  | T4 for UDP<br>0s for TCP/SCTP    | T4 for UDP<br>0s for TCP/SCTP                 | Wait time for response retransmits   |
| NOTE:     | As a network option, SIP T1 Timer's value can be extended, along with the necessary modifications of T2 and T4 Timers' values, to take into account the specificities of the supported services when the MRFC and the controlling AS are under the control of the same operator and the controlling AS knows, based on local configuration, that the MRFC implements a longer value of SIP T1 Timer. |                                  |   |  |

## 7.8 IM CN subsystem timers

Table 7.8.1 shows recommended values for timers specific to the IM CN subsystem.

Table 7.8.1: IM CN subsystem

| Timer          | Value to be applied at the UE | Value to be applied at the P-CSCF | Value to be applied at the S-CSCF | Meaning  |
|----------------|-------------------------------|-----------------------------------|-----------------------------------|--|
| reg-await-auth | not applicable                | not applicable                    | 4 minutes                         | The timer is used by the S-CSCF during the authentication procedure of the UE. For detailed usage of the timer see subclause 5.4.1.2.<br>The authentication procedure may take in the worst case as long as 2 times Timer F. The IM CN subsystem value for Timer F is 128 seconds. |

NOTE: The UE and the P-CSCF use the value of the reg-await-auth timer to set the SIP level lifetime of the temporary set of security associations.

## 7.9 Media feature tags defined within the current document

### 7.9.1 General

This subclause describes the media feature tag definitions that are applicable for the 3GPP IM CN subsystem.

## 7.9.2 Definition of media feature tag g.3gpp.icsi-ref

Media feature-tag name: g.3gpp.icsi-ref.

ASN.1 Identifier: 1.3.6.1.8.2.4

Summary of the media feature indicated by this tag: Each value of the Service Reference media feature-tag indicates the software applications supported by the agent. The values for this tag equal the IMS communication Service Identifier (ICSI) values supported by the agent.

The Service Reference media feature tag is defined to fulfil the requirements for forking to an appropriate UE when multiple UEs are registered and dispatch to an appropriate application within the UE based upon the IMS communication Service Identifier (ICSI) values as stated in 3GPP TS 23.228 [7].

Multiple tag-values can be included in the Service Reference media feature-tag.

Values appropriate for use with this feature-tag: Token with an equality relationship.

The feature-tag is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms:

This feature-tag is most useful in a communications application, for describing the capabilities of a device, such as a phone or PDA.

Examples of typical use: Routeing an IMS Communication Session to a device that supports a particular software application or understands a particular service.

Related standards or documents:

3GPP TS 24.229: "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), stage 3"

Security Considerations: Security considerations for this media feature-tag are discussed in subclause 11.1 of RFC 3840 [62].

## 7.9.3 Definition of media feature tag g.3gpp.iari-ref

Media feature-tag name: g.3gpp.iari-ref.

ASN.1 Identifier: 1.3.6.1.8.2.5

Summary of the media feature indicated by this tag: Each value of the Application Reference media feature-tag indicates the software applications supported by the agent. The values for this tag equal IMS Application Reference Identifier (IARI) values supported by the agent

The Application Reference media feature tag is defined to fulfil the requirements for forking to an appropriate UE when multiple UEs are registered and dispatch to an appropriate application within the UE based upon and IMS Application Reference Identifier (IARI) values as stated in 3GPP TS 23.228 [7].

Multiple tag-values can be included in the Application Reference media feature-tag.

Values appropriate for use with this feature-tag: Token with an equality relationship.

The feature-tag is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms:

This feature-tag is most useful in a communications application, for describing the capabilities of a device, such as a phone or PDA.

Examples of typical use: Routeing an IMS Application Session to a device that supports a particular software application or understands a particular application.

Related standards or documents:

3GPP TS 24.229: "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), stage 3"

Security Considerations: Security considerations for this media feature-tag are discussed in subclause 11.1 of RFC 3840 [62].

7.9.4 Void

7.9.5 Void

7.9.6 Void

## 7.9A Feature-capability indicators defined within the current document

### 7.9A.1 General

This subclause describes the feature-capability indicators definitions, according to RFC 6809 [190], that are applicable for the 3GPP IM CN subsystem.

### 7.9A.2 Definition of feature-capability indicator g.3gpp.icsi-ref

Feature-capability indicator name: g.3gpp.icsi-ref.

Summary of the feature indicated by this feature-capability indicator: Each value of the Service Reference feature-capability indicator indicates the software applications supported by the entity. The values for this feature-capability indicator equal the IMS communication Service Identifier (ICSI) values supported by the entity.

Multiple feature-capability indicator values can be included in the Service Reference feature-capability indicators.

When included in the Feature-Caps header field, according to RFC 6809 [190], the value of this feature-capability indicator contains the IMS communication service identifier (ICSI) of the IMS communication service supported for use:

- in the standalone transaction (if included in a request for a standalone transaction or a response associated with it); or
- in the dialog (if included in an initial request for dialog or a response associated with it);

by the entity which included the Feature-Caps header field.

Feature-capability indicator specification reference: 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

Values appropriate for use with this feature-capability indicator:

When used in a Feature-Caps header field, the g.3gpp-icsi-ref feature-capability indicator is encoded using the feature-cap header field rules specified in clause 6.3 of RFC 6809 [190], where the feature-capability indicator value is an instance of fcap-value-list, listing one or more token values, as specified in RFC 6809 [190].

Examples of typical use: Indicating support of IMS Communication Services to other network entities.

Security Considerations: Security considerations for this feature-capability indicator are discussed in clause 9 of RFC 6809 [190].

### 7.9A.3 Definition of feature-capability indicators g.3gpp.trf

Feature-capability indicator name: g.3gpp.trf

Summary of the feature indicated by this feature-capability indicator:

This feature-capability indicator, when included in a Feature-Caps header field as specified in RFC 6809 [190] in a SIP INVITE request, indicates that in a roaming scenario, the visited network supports a transit and roaming functionality in order to allow loopback of session requests to the visited network from the home network. When used, it may indicate the URI of the transit and roaming functionality.

Feature-capability indicator specification reference: 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

Values appropriate for use with this feature-capability indicator:

None or string with an equality relationship. When used in a Feature-Caps header field, the value is string and follows the syntax as described in table 7.9A.1 for g-3gpp-trf. The value of g-3gpp-trf parameter is an instance of fcap-string-value of Feature-Caps header field specified in RFC 6809 [190].

**Table 7.9A.1: ABNF syntax of values of the g.3gpp.trf feature-capability indicator**

```
g-3gpp-trf = "<" SIP-URI ">"
```

The feature-capability indicator is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms: This feature-capability indicator is used to indicate visited network support of the roaming architecture for voice over IMS with local breakout and to transport the TRF address.

Examples of typical use: A visited network indicating the presence and support of a TRF in a visited network to the home network.

Security Considerations: Security considerations for this feature-capability indicator are discussed in clause 9 of RFC 6809 [190].

#### 7.9A.4 Definition of feature-capability indicator g.3gpp.loopback

Feature-capability indicator name: g.3gpp.loopback

Summary of the feature indicated by this feature-capability indicator:

This feature-capability indicator, when included in a Feature-Caps header field as specified in RFC 6809 [190] in a SIP INVITE request, indicates the support of the roaming architecture for voice over IMS with local breakout.

Feature-capability indicator specification reference: 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

Values appropriate for use with this feature-capability indicator:

None or a string with an equality relationship.

When used in a Feature-Caps header field, the value is a string identifying the home network and follows the syntax as described in table 7.9A.4-1 for g-3gpp-loopback. The value of g-3gpp-loopback parameter is an instance of fcap-string-value of Feature-Caps header field specified in RFC 6809 [190].

**Table 7.9A.4-1: ABNF syntax of values of the g-3gpp-loopback feature-capability indicator**

```
g-3gpp-loopback = "<" 1*(qdttext / quoted-pair) ">"
```

The feature-capability indicator is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms: This feature-capability indicator is used to indicate support of the roaming architecture for voice over IMS with local breakout and that the INVITE request is a loopback request.

Examples of typical use: The home network indicating when a loopback INVITE request is sent to a visited network.

Security Considerations: Security considerations for this feature-capability indicator are discussed in clause 9 of RFC 6809 [190].

#### 7.9A.5 Definition of feature-capability indicator g.3gpp.home-visited

Feature-capability indicator name: g.3gpp.home-visited

Summary of the feature indicated by this feature-capability indicator:

This feature-capability indicator, when included in a Feature-Caps header field as specified in RFC 6809 [190] in a SIP INVITE request, indicates that the home network supports loopback to the identified visited network for this session. The loopback is expected to be applied at some subsequent entity to the insertion point. The feature-capability indicator carries a parameter value which indicates the visited network.

Feature-capability indicator specification reference: 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

Values appropriate for use with this feature-capability indicator:

String with an equality relationship. When used in a Feature-Caps header field, the value follows the syntax as described in table 7.9A.2 for g-3gpp-home-visited. The value of g-3gpp-home-visited parameter is an instance of fcap-string-value of Feature-Caps header field specified in RFC 6809 [190].

**Table 7.9A.2: ABNF syntax of values of the g.3gpp.home-visited feature-capability indicator**

```
g-3gpp-home-visited = "<" 1*(qdttext / quoted-pair) ">"
```

The value follows that used in the P-Visited-Network-ID header field.

The feature-capability indicator is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms: This feature-capability indicator is used to indicate the home network supports loopback to the identified visited network for this session. The loopback is expected to be applied at some subsequent entity to the insertion point. The feature-capability indicator carries a parameter which indicates the visited network.

Examples of typical use: A home network indicating the home network supports loopback to the identified visited network for this session.

Security Considerations: Security considerations for this feature-capability indicator are discussed in clause 9 of RFC 6809 [190].

## 7.9A.6 Definition of feature-capability indicator g.3gpp.mrb

Feature-capability indicator name: g.3gpp.mrb

Summary of the feature indicated by this feature-capability indicator:

This feature-capability indicator when included in a Feature-Caps header field as specified in RFC 6809 [190] in a SIP INVITE request indicates that in a roaming scenario, the visited network supports media resource broker functionality for the allocation of multimedia resources in the visited network. When used, it indicates the URI of the visited network MRB.

Feature-capability indicator specification reference:

3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

Values appropriate for use with this feature-capability indicator:

String with an equality relationship. When used in a Feature-Caps header field, the value is string and follows the syntax as described in table 7.9A.3 for g-3gpp-mrb. The value of g-3gpp-mrb parameter is an instance of fcap-string-value of Feature-Caps header field specified in RFC 6809 [190].

**Table 7.9A.3: ABNF syntax of values of the g.3gpp.mrb feature-capability indicator**

```
g-3gpp-mrb = "<" SIP-URI ">"
```

The feature-capability indicator is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms: This feature-capability indicator is used to indicate the URI of the media resource broker.

Examples of typical use: Indicating the URI of the visited network MRB to the home network.

Security Considerations: Security considerations for this feature-capability indicator are discussed in clause 9 of draft-ietf-sipcore-proxy-feature [190].

## 7.10 Reg-event package extensions defined within the current document

### 7.10.1 General

This subclause describes the reg-event package extensions that are applicable for the IM CN subsystem.

### 7.10.2 Reg-Event package extension to transport wildcarded public user identities

#### 7.10.2.1 Structure and data semantics

This subclause defines an extension to the event registration package (RFC 3680 [43]) to transport policy to transport wildcarded public user identities that are encoded using regular expression.

In order to include a wildcarded public user identity in the event registration package, the notifier shall

1. if the registration set of the identity whose registration status is notified contains a wildcarded public user identity, add a <wildcardedIdentity> sub-element defined in subclause 7.10.2.2 of this document to the <registration> element of the wildcarded identity;
2. for the <registration> element containing a <wildcardedIdentity> sub-element:
  - a) set the aor attribute to any public user identity that is represented by the wildcarded identity; and
  - b) set the <wildcardedIdentity> sub-element inside of the <registration> element to the wildcarded identity as received via the Cx interface.

NOTE: The public user identity that is put into the aor attribute does not have any extra privileges over any other public user identity that is represented by a wildcarded public user identity.

#### 7.10.2.2 XML Schema

Table 7.10.1 in this subclause defines the XML Schema describing the extension to transport wildcarded public user identities which can be included in the reg event package sent from the S-CSCF in NOTIFY requests.

**Table 7.10.1: Wildcarded Identity, XML Schema**

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:3gpp:ns:extRegExp:1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:element name="wildcardedIdentity" type="xs:string"/>
</xs:schema>
```

NOTE: Multiple wildcarded elements can be included in one registration element.

### 7.10.3 Reg-event package extension for policy transport

#### 7.10.3.1 Scope

This subclause describes coding which extends the registration event package defined in RFC 3680 [43] to transport policy associated with a public user identity.

#### 7.10.3.2 Structure and data semantics

The policy associated with a public user identity shall be encoded as follows:

1. add an <actions> element defined in the RFC 4745 [182] in the <registration> element of the public user identity in the registration information;

NOTE: The <actions> element is validated by the <xs:any namespace="##other" processContents="lax" minOccurs="0" maxOccurs="unbounded"/> particle of the <registration> elements.

2. if the policy to the usage of the communication resource priority (see RFC 4412 [116]) is associated with the public user identity, then for each allowed usage:
  - a. include <rph> child element in the <actions> child element of the <registration> element;
  - b. set the 'ns' attribute of the <rph> child element of the <actions> child element of the <registration> element to the allowed resource priority namespace as specified in RFC 4412 [116] and as registered in IANA; and
  - c. set the 'val' attribute of the <rph> child element of the <actions> child element of the <registration> element to the allowed resource priority value within the allowed resource priority namespace;
3. if the policy to act as privileged sender (the P-CSCF passes identities for all calls) is associated with the public user identity, then include a <privSender> child element in the <actions> child element of the <registration> element;
4. if the policy for special treatment of the P-Private-Network-Indication header field (the P-CSCF allows the UE to make private calls) is associated with the public user identity, then include a <pni> child element in the <actions> child element of the <registration> element, and shall:
  - a. if a P-Private-Network-Indication header field shall be forwarded, if received from the attached equipment, set the "insert" attribute of the <pni> element to a "fwd" value;
  - b. if a P-Private-Network-Indication header field shall be inserted in all requests received from the attached equipment, insert an "insert" attribute of the <pni> element to a "ins" value; and
  - c. if the value of the "insert" attribute is "ins", insert a "domain" attribute with the value of the URI to be set in the P-Private-Network-Indication header field; and
5. if the policy to act as privileged sender for the calls with the P-Private-Network-Indication header field (the P-CSCF allows the UE to make private calls, and the P-CSCF passes identities only for private calls) is associated with the public user identity, then include a <privSenderPNI> child element in the <actions> child element of the <registration> element.

NOTE: If only the <privSender> child element is sent and no <privSenderPNI> child element is sent, then the <privSender> child element applies to both public network traffic and private network traffic (i.e. that with special treatment of the P-Private-Network-Indication header field).

### 7.10.3.3 XML Schema

Table 7.10.2 in this subclause defines the XML Schema describing the individual policies which can be delivered to the P-CSCF or UE using the reg event package extension for policy transport.

**Table 7.10.2: Reg event package extension for policy transport, XML Schema**

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:3gpp:ns:extRegInfo:1.0"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xs:element name="rph">
    <xs:complexType>
      <xs:attribute name="ns" type="xs:string"/>
      <xs:attribute name="val" type="xs:string"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="privSender">
    <xs:complexType/>
  </xs:element>
  <xs:element name="pni">
    <xs:complexType>
      <xs:attribute name="insert">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="fwd"/>
            <xs:enumeration value="ins"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:attribute>
      <xs:attribute name="domain" type="xs:anyURI"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="privSenderPNI">
    <xs:complexType/>
  </xs:element>
</xs:schema>

```

## 7.11 Void

## 7.12 Info package definitions and associated MIME type definitions

### 7.12.1 DTMF info package and session-info MIME type

#### 7.12.1.1 DTMF info package

##### 7.12.1.1.1 General

This subclause contains the information required for the IANA registration of an info package.

The digit message body and associated MIME type can also be used as defined in other specifications in a legacy manner as defined by RFC 6086 [25].

##### 7.12.1.1.2 Overall description

DTMF tones are normally sent when a user presses a button on the terminal. Each tone, identified by a unique frequency, represents a number (0-9) or a special character. The DTMF info package is used to transport that value. In-order delivery of the DTMF digits is not controlled by the DTMF info package, this would be controlled either by queuing in the sender or by separate interaction with the human user; such mechanisms are out of scope of this registration.

The DTMF info package can be used to transport a single DTMF tone, or a series of tones. If a series of tones is transported in a single SIP INFO request, it is not possible to indicate the duration between each tone in the series.

The DTMF info package is not defined for a specific application. Any application, where sending of DTMF tones using the SIP INFO method is required, can use the DTMF info package.



### 7.12.1.1.3 Applicability

The info package mechanism for transporting DTMF tones has been chosen because it allows SIP entities that do not have access to the user plane (where DTMF tones can also be transported) to send and receive tones. The mechanism also allows the tones to be sent inside an existing dialog, using the same signalling path as other SIP messages within the dialog, rather than having to establish a separate dialog (DTMF tones can also be transported using subscription event packages).

### 7.12.1.1.4 Info package name

The name of the DTMF info package is: infoDtmf

### 7.12.1.1.5 Info package parameters

No parameters are defined for the DTMF info package.

### 7.12.1.1.6 SIP option tags

No SIP option tags are defined for the DTMF info package.

### 7.12.1.1.7 INFO message body parts

The DTMF digits are carried in the Overlap digit message body, defined in subclause 7.12.1.2.

The MIME type value for the message body is "application/session-info", defined in subclause 7.12.1.2.

The Content Disposition value for the message body, when associated with the DTMF info package, is "info-package" (see RFC 6086 [25]).

### 7.12.1.1.8 Info package usage restrictions

No usage restrictions are defined for the DTMF info package.

If SIP entities support multiple mechanisms for sending DTMF tones they need to ensure, using negotiation mechanisms, that each entity is aware of which mechanism is used.

### 7.12.1.1.9 Rate of INFO requests

No maximum rate or minimum rate is defined for sending INFO requests associated with the DTMF info package.

When DTMF tones are triggered by user interaction, the DTMF tones are normally generated when the user pushes a button. Specific applications can decide upon which rate DTMF tones are generated. However, the DTMF info package does not provide a feedback mechanism to indicate to the sender that the rate of DTMF tones is too slow or fast.

### 7.12.1.1.10 Info package security considerations

No additional security mechanism is defined for the DTMF info package.

The security of the DTMF info package is based on the generic security mechanism provided for the underlying SIP signalling.

The mechanism should not be used for transferring any data that requires a greater level of security than the underlying SIP signalling.

## 7.12.1.2 Overlap digit message body

### 7.12.1.2.1 Scope

This section defines a message body that shall be used for sending additional digits, which have not previously been sent, in SIP INFO messages ("legacy" mode of usage of the INFO method as defined in IETF RFC 6086 [133]) when the in-dialog method is used for overlap dialling.

The same message body can also be used for transporting Dual Tone Multi Frequency (DTMF) tones using SIP INFO requests, using the DTMF info package (see RFC 6086 [25]) defined in subclause 7.12.1.1.

The support of this message body is a network option.

#### 7.12.1.2.2 MIME type

The message body defined in the present Annex is registered at IANA as "application/session-info" MIME type.

If the message body is embedded in SIP INFO messages, the Content-Type header shall be set to "application/session-info" and the Content-Disposition header shall be set to "signal" with the handling parameter set to "optional".

#### 7.12.1.2.3 ABNF

session-info = SubsequentDigit

SubsequentDigit = "SubsequentDigit" HCOLON phonedigits

phonedigits = 1\*(HEXDIG / "\*" / "#")

HEXDIG = DIGIT / "A" / "B" / "C" / "D" / "E" / "F"

#### 7.12.1.2.4 IANA registration template

Within the present subclause, information required for an IANA registration at <http://www.iana.org/cgi-bin/mediatypes.pl> is provided.

##### 1. Media Type Name

Application

##### 2. Subtype name

"session-info" (Standards Tree)

##### 3. Required parameters

none

##### 4. Optional parameters

none

##### 5. Encoding considerations

binary

##### 6. Security considerations

Modifications of the MIME body by a man-in-the-middle can have severe consequences:

The overlap digits that can be transported with this MIME body influence the routing of the SIP session that is being setup.

Dual Tone Multi Frequency (DTMF) tones that can also be transported with this MIME body will be interpreted by the application of the end points of the communication for various purposes.

However, this MIME body is used only attached to SIP INFO messages, and modifications of other parts of the SIP signalling will lead to comparable consequences. Protection of the SIP signalling will also protect the present MIME body.

The information transported in this MIME media type does not include active or executable content.

Mechanisms for privacy and integrity protection of protocol parameters exist. Those mechanisms as well as authentication and further security mechanisms are described in 3GPP TS 24.229.

##### 7. Interoperability considerations

none

##### 8. Published specification

3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), stage 3".

#### 9. Applications which use this media type

This MIME type is used as a message body within SIP INFO messages.

It is either used for sending additional digits of the callee's number, which have not previously been sent, in SIP INFO messages ("legacy" mode of usage of the INFO method as defined in RFC 6086 [25]) when the in-dialog method is used for overlap dialling.

The same message body can also be used for transporting Dual Tone Multi Frequency (DTMF) tones using SIP INFO requests, using the DTMF info package (see RFC 6086 [25]) defined in subclause 7.12.1.1.

#### 10. Additional information

Magic number(s): none

File extension(s): none

Macintosh File Type Code(s): none

Object Identifier(s) or OID(s): none

#### 11. Intended usage

Limited Use

#### 12. Other Information/General Comment

none.

### 7.12.1.3 Implementation details and examples

Examples of the DTMF info package usage can be found in the following specification:

- 3GPP TS 24.182 [8Q]: "Customized Alerting Tones; Protocol specification".

---

## 8 SIP compression

### 8.1 SIP compression procedures at the UE

#### 8.1.1 SIP compression

If in normal operation the UE generates requests or responses containing a P-Access-Network-Info header field which included a value of "3GPP-GERAN", "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP-E-UTRAN-FDD", "3GPP-E-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "3GPP2-UMB", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", "IEEE-802.11g", "IEEE-802.11n", or "DVB-RCS2", then the UE shall support:

- SigComp as specified in RFC 3320 [32] and as updated by RFC 4896 [118]; and
- the additional requirements specified in RFC 5049 [79], with the exception that the UE shall take a State Memory Size of at least 4096 bytes as a minimum value.

If in normal operation the UE generates requests or responses containing a P-Access-Network-Info header field which included a value of "3GPP-GERAN", "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP-E-UTRAN-FDD", "3GPP-E-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "3GPP2-UMB", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", "IEEE-802.11g", "IEEE-802.11n", or "DVB-RCS2", then the UE may support:

- the negative acknowledgement mechanism specified in RFC 4077 [65A].

When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486 [55]. When the UE will create the compartment is implementation specific, but the compartment shall not be created until a set of security associations or a TLS session is set up if signalling security is in use. The UE shall finish the compartment when the UE

is deregistered. The UE shall allow state creations and announcements only for messages received in a security association.

NOTE: Exchange of bytecodes during registration will prevent unnecessary delays during session setup.

If the UE supports SigComp:

- the UE shall support the SIP dictionary specified in RFC 3485 [42] and as updated by RFC 4896 [118]. If compression is enabled, the UE shall use the dictionary to compress the first message; and
- if the UE supports the presence user agent or watcher roles as specified in table A.3A/2 and table A.3A/4, the UE may support the presence specific dictionary specified in RFC 5112 [119].

The use of SigComp is not re-negotiated between initial registration and deregistration.

## 8.1.2 Compression of SIP requests and responses transmitted to the P-CSCF

In normal operation the UE should send the generated requests and responses transmitted to the P-CSCF:

- compressed according to subclause 8.1.1, if the P-Access-Network-Info header field of the initial registration message includes a value of "3GPP-GERAN", "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "3GPP2-UMB", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", "IEEE-802.11g", "IEEE-802.11n", or "DVB-RCS2";
- uncompressed, if the P-Access-Network-Info header field of the initial registration message includes a value of "3GPP-E-UTRAN-FDD" or "3GPP-E-UTRAN-TDD".

In other cases where SigComp is supported, the UE need not compress the requests and responses.

NOTE 1: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

NOTE 2: In an IP-CAN where compression support is mandatory the UE can send even the first message compressed. Sigcomp provides mechanisms to allow the UE to know if state has been created in the P-CSCF or not.

## 8.1.3 Decompression of SIP requests and responses received from the P-CSCF

If the UE supports SigComp, then the UE shall decompress the compressed requests and responses received from the P-CSCF according to subclause 8.1.1.

NOTE: According to RFC 3486 [55], the UE not supporting SigComp or not indicating willingness to receive compressed messages never receives compressed SIP messages.

If the UE detects a decompression failure at the P-CSCF, the recovery mechanism is implementation specific.

# 8.2 SIP compression procedures at the P-CSCF

## 8.2.1 SIP compression

The P-CSCF shall support:

- SigComp as specified in RFC 3320 [32] and as updated by RFC 4896 [118]; and
- the additional requirements specified in RFC 5049 [79], with the exception that the P-CSCF shall take a State Memory Size of at least 4096 bytes as a minimum value.

The P-CSCF may support:

- the negative acknowledgement mechanism specified in RFC 4077 [65A].

When using SigComp the P-CSCF shall send compressed SIP messages in accordance with RFC 3486 [55]. When the P-CSCF will create the compartment is implementation specific, but the compartment shall not be created until a set of security associations are set up. The P-CSCF shall finish the compartment when the UE is deregistered. The P-CSCF shall allow state creations and announcements only for messages received in a security association.

The P-CSCF:

- shall support the SIP dictionary specified in RFC 3485 [42] and as updated by RFC 4896 [118]. If compression is enabled, the P-CSCF shall use the dictionary to compress the first message; and
- may support the presence specific dictionary specified in RFC 5112 [119].

NOTE: Exchange of bytecodes during registration will prevent unnecessary delays during session setup.

## 8.2.2 Compression of SIP requests and responses transmitted to the UE

For all SIP transactions on a specific security association where the security association was established using a REGISTER request from the UE containing a P-Access-Network-Info header field which included a value of "3GPP-GERAN", "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP-E-UTRAN-FDD", "3GPP-E-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "3GPP2-UMB", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", "IEEE-802.11g", "IEEE-802.11n", or "DVB-RCS2", and the UE has indicated that it supports SigComp and is willing to receive compressed messages in accordance with RFC 3486 [55], then the P-CSCF should compress the requests and responses transmitted to the UE according to subclause 8.2.1. In other cases where SigComp is supported, it need not.

NOTE: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

## 8.2.3 Decompression of SIP requests and responses received from the UE

The P-CSCF shall decompress the compressed requests and responses received from the UE according to subclause 8.2.1.

If the P-CSCF detects a decompression failure at the UE, the recovery mechanism is implementation specific.

---

# 9 IP-Connectivity Access Network aspects when connected to the IM CN subsystem

## 9.1 Introduction

A UE accessing the IM CN subsystem and the IM CN subsystem itself utilises the services supported by the IP-CAN to provide packet-mode communication between the UE and the IM CN subsystem. General requirements for the UE on the use of these packet-mode services are specified in this clause.

Possible aspects particular to each IP-CAN is described separately for each IP-CAN.

## 9.2 Procedures at the UE

### 9.2.1 Connecting to the IP-CAN and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

- a) establish a connection with the IP-CAN;
- b) obtain an IP address using either the standard IETF protocols (e.g., DHCP or IPCP) or a protocol that is particular to the IP-CAN technology that the UE is utilising. The UE shall fix the obtained IP address throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the last deregistration; and
- c) acquire a P-CSCF address(es).

The UE may acquire an IP address via means other than the DHCP. In this case, upon acquiring an IP address, the UE shall request the configuration information (that includes the DNS and P-CSCF addresses) from the DHCP server.

The methods for acquiring a P-CSCF address(es) are:

- I. Employ Dynamic Host Configuration Protocol for IPv4 RFC 2131 [40A] or for IPv6 (DHCPv6) RFC 3315 [40]. Employ the DHCP options for SIP servers RFC 3319 [41] or, for IPv6, RFC 3361 [35A]. Employ the DHCP options for Domain Name Servers (DNS) RFC 3646 [56C].

The UE shall either:

- in the DHCP query, request a list of SIP server domain names of P-CSCF(s) and the list of Domain Name Servers (DNS); or
  - request a list of SIP server IP addresses of P-CSCF(s).
- II. Obtain the P-CSCF address(es) by employing a procedure that the IP-CAN technology supports. (e.g. GPRS).
  - III. The UE may use pre-configured P-CSCF address(es) (IP address or domain name). For example:
    - a. The UE selects a P-CSCF from the list stored in ISIM or IMC;
    - b. The UE selects a P-CSCF from the list in IMS management object.

NOTE: Access-specific annexes provide additional guidance on the method to be used by the UE to acquire P-CSCF address(es).

When acquiring a P-CSCF address(es), the UE can freely select either method I or II or III.

The UE may also request a DNS Server IP address(es) as specified in RFC 3315 [40] and RFC 3646 [56C] or RFC 2131 [40A].

## 9.2.2 Handling of the IP-CAN

The means to ensure that appropriate resources are available for the media flow(s) on the IP-CAN(s) related to a SIP session is dependant on the characteristics for each IP-CAN, and is described separately for each IP-CAN in question.

GPRS is described in annex B. I-WLAN is described in annex D. xDSL is described in annex E. DOCSIS is described in Annex H. EPS is described in annex L. cdma2000<sup>®</sup> packet data subsystem is described in Annex M. EPC via cdma2000<sup>®</sup> HRPD is described in annex O. cdma2000<sup>®</sup> Femtocell network is described in annex Q. DVB-RCS2 is described in Annex S. If a particular handling of the IP-CAN is needed for emergency calls, this is described in the annex for each access technology.

### 9.2.2A P-CSCF restoration procedure

The UE may support P-CSCF restoration procedures.

An IP-CAN may provide means for detecting a P-CSCF failure.

An UE supporting the P-CSCF restoration procedure should either use the keep-alive procedures described in RFC 6223 [143] or the procedure provided by a IP-CAN for monitoring the P-CSCF status.

NOTE 1: The UE can use other means to monitor the P-CSCF status, e.g. ICMP echo request/response. However, those other means are out of scope of this document.

NOTE 2: A UE registered through the procedures described in RFC 5626 [92] can use the keep-alive mechanism to monitor the status of the P-CSCF.

### 9.2.3 Special requirements applying to forked responses

Since the UE does not know that forking has occurred until a second provisional response arrives, the UE will request the radio/bearer resources as required by the first provisional response. For each subsequent provisional response that may be received, different alternative actions may be performed depending on the requirements in the SDP answer:

- the UE has sufficient radio/bearer resources to handle the media specified in the SDP of the subsequent provisional response, or
- the UE must request additional radio/bearer resources to accommodate the media specified in the SDP of the subsequent provisional response.

NOTE 1: When several forked responses are received, the resources requested by the UE is the "logical OR" of the resources indicated in the multiple responses to avoid allocation of unnecessary resources. The UE does not request more resources than proposed in the original INVITE request.

NOTE 2: When service-based local policy is applied, the UE receives the same authorization token for all forked requests/responses related to the same SIP session.

When an 199 (Early Dialog Terminated) response for the INVITE request is received for an early dialogue, the UE shall release reserved radio/bearer resources associated with that early dialogue.

When the first final 200 (OK) response for the INVITE request is received for one of the early dialogues, the UE proceeds to set up the SIP session using the radio/bearer resources required for this session. Upon the reception of the first final 200 (OK) response for the INVITE request, the UE shall release all unneeded radio/bearer resources.

---

## 10 Media control

### 10.1 General

The choice of which media control methods below to use is service specific, it depends on the functionality required and physical deployment architectures.

Combinations of the capabilities below are supported by the use of the control channel framework RFC 6230 [146] with associated media control packages.

For security, the principles and protocols described in 3GPP TS 33.210 [19A] shall take precedence over those specified in the referenced specifications in this clause.

For codecs, those described in access specific specifications shall take precedence over those specified in the referenced specifications in this clause.

### 10.2 Procedures at the AS

#### 10.2.1 General

An AS requesting charging information and authorisation for specific media operations and media usage controlled by the MRFC shall use RFC 6230 [146] together with appropriate packages.

NOTE: This is in addition to the charging related procedures in clause 5 and to the charging information and authorisation requests, defined in 3GPP TS 32.260 [17] which provide charging information and authorisation for SIP session and SDP information.

An AS may support delegation of an XML (such as CCXML or SCXML) script execution to an MRFC. An AS supporting delegation of XML script execution shall use RFC 6230 [146] together with appropriate packages.

The packages, or extensions to existing packages using RFC 6230 [146] framework are not specified in this release.

The AS may support the media server resource consumer interface as defined by RFC 6917 [192]. If supported the AS can support either the in-line mode or the query mode or both.

#### 10.2.2 Tones and announcements

##### 10.2.2.1 General

An AS may support control of the MRFC for tones and announcements. An AS supporting control of the MRFC for tones and announcements shall support one or more of the following methods:

- RFC 4240 [144] announcement service;

- RFC 5552 [145]; or
- RFC 6230 [146] and RFC 6231 [147].

### 10.2.2.2 Basic network media services with SIP

The AS may support control of the MRFC for basic announcements by the use of RFC 4240 [144] and the announcement service described in RFC 4240 [144] subclause 3.

The media control commands are carried between the AS and the MRFC either directly over the Mr' interface or via the S-CSCF over the ISC and Mr interfaces.

The AS shall provide remote prompts to the MRFC using the AS-MRFC Cr interface.

### 10.2.2.3 SIP interface to VoiceXML media services

The AS may support control of the MRFC for voice dialogs by the use of RFC 5552 [145].

The media control commands are carried between the AS and the MRFC either directly over the Mr' interface or via the S-CSCF over the ISC and Mr interfaces.

The AS shall provide remote prompts and scripts to the MRFC using the AS-MRFC Cr interface.

Data shall be returned to the AS from the MRFC by either use of the AS-MRFC Cr interface (subclause 4.1 of RFC 5552 [145]), via the ISC interface (subclause 4.2 of RFC 5552 [145]) or via the Mr' interface.

### 10.2.2.4 Media control channel framework and packages

The AS may support control of the MRFC for interactive voice response by the use of RFC 6231 [147] and RFC 6230 [146].

The AS shall provide remote prompts, media control commands and scripts to the MRFC using the AS-MRFC Cr interface.

The AS shall implement the control client role as described in RFC 6230 [146].

## 10.2.3 Ad-hoc conferences

### 10.2.3.1 General

An AS may support control of the MRFC for ad-hoc conferencing. An AS supporting control of the MRFC for ad-hoc conferencing shall support one or more of the following methods:

- RFC 4240 [144] conference service; or
- RFC 6230 [146] and RFC 6505 [148].

### 10.2.3.2 Basic network media services with SIP

The AS may support control of the MRFC for basic conferencing by the use of RFC 4240 [144] and the conference service described in RFC 4240 [144] subclause 5.

The media control commands are carried between the AS and the MRFC either directly over the Mr' interface or via the S-CSCF over the ISC and Mr interfaces.

### 10.2.3.3 Media control channel framework and packages

The AS may support control of the MRFC for conference mixing by the use of RFC 6505 [148] and RFC 6230 [146].

An AS may support control of the MRFC for floor controlled conferences (as specified in 3GPP TS 24.147 [8B]), via the use of RFC 6230 [146] together with appropriate packages. The packages, or extensions to existing packages using RFC 6230 [146] framework are not specified in this release.

An AS may support control of the MRFC for session-mode messaging conferences (as specified in 3GPP TS 24.247 [8F]), via the use of RFC 6230 [146] together with appropriate packages. The packages, or extensions to existing packages using RFC 6230 [146] framework are not specified in this release.



The AS shall provide media control commands to the MRFC using the AS-MRFC Cr interface.

The AS shall implement the control client role as described in RFC 6230 [146].

## 10.2.4 Transcoding

### 10.2.4.1 General

An AS may support control of the MRFC for transcoding. An AS supporting control of the MRFC for transcoding shall support one or more of the following methods:

- RFC 4240 [144] conference service; or
- RFC 6230 [146] and RFC 6505 [148].

### 10.2.4.2 Basic network media services with SIP

The AS may support control of the MRFC for transcoding by the use of RFC 4240 [144] and the conference service described in RFC 4240 [144] subclause 5.

The media control commands are carried between the AS and the MRFC either directly over the Mr' interface or via the S-CSCF over the ISC and Mr interfaces.

### 10.2.4.3 Media control channel framework and packages

The AS may support control of the MRFC for transcoding by the use of RFC 6505 [148] and RFC 6230 [146].

The AS shall provide media control commands to the MRFC using the AS-MRFC Cr interface.

The AS shall implement the control client role as described in RFC 6230 [146].

## 10.3 Procedures at the MRFC

### 10.3.1 General

An MRFC required to generate charging information and authorize requests from an AS for specific media operations and media usage shall support RFC 6230 [146] together with appropriate packages.

**NOTE:** This is in addition to the charging related procedures in clause 5 and to the charging information and authorisation requests, defined in 3GPP TS 32.260 [17] which provide charging information and authorisation for SIP session and SDP information.

An MRFC may support delegated XML (such as CCXML or SCXML) script execution from an AS. An MRFC supporting delegation of XML script execution shall use RFC 6230 [146] together with appropriate packages.

The packages, or extensions to existing packages using RFC 6230 [146] framework above are not specified in this release.

The MRFC may support the media server resource publish interface as defined by RFC 6917 [192].

### 10.3.2 Tones and announcements

#### 10.3.2.1 General

An MRFC may support control of tones and announcements. An MRFC supporting control of tones and announcements shall support one or more of the following methods:

- RFC 4240 [144] announcement service;
- RFC 5552 [145]; or
- RFC 6230 [146] and RFC 6231 [147].

### 10.3.2.2 Basic network media services with SIP

The MRFC may support control of basic announcements by the use of RFC 4240 [144] and the announcement service described in RFC 4240 [144] subclause 3.

The media control commands are received from the AS either directly over the Mr' interface or via the S-CSCF over the ISC and Mr interfaces.

The MRFC shall fetch remote prompts from the AS using the AS-MRFC Cr interface.

The MRFC acts as the media server described in RFC 4240 [144].

### 10.3.2.3 SIP interface to VoiceXML media services

The MRFC may support control of voice dialogs by the use of RFC 5552 [145].

The media control commands are received from the AS either directly over the Mr' interface or via the S-CSCF over the ISC and Mr interfaces.

The MRFC shall fetch via the AS-MRFC Cr interface the remote prompts and scripts from the address included in the "voicexml" URI parameter, if received, in the Request-URI of the SIP INVITE request.

Data shall be returned to the AS from the MRFC by either use of the AS-MRFC Cr interface (subclause 4.1 of RFC 5552 [145]), via the ISC interface (subclause 4.2 of RFC 5552 [145]) or via the Mr' interface.

The MRFC acts as the VoiceXML media server described in RFC 5552 [145].

### 10.3.2.4 Media control channel framework and packages

The MRFC may support control of interactive voice response by the use of RFC 6231 [147] and RFC 6230 [146].

The MRFC shall fetch remote prompts and scripts from the MRFC using the AS-MRFC Cr interface. The MRFC shall send media control command responses and notifications to the AS using the AS-MRFC Cr interface.

The MRFC shall implement the control server role as described in RFC 6230 [146].

## 10.3.3 Ad-hoc conferences

### 10.3.3.1 General

An MRFC may support control of ad-hoc conferencing. An MRFC supporting control of ad-hoc conferencing shall support one or more of the following methods:

- RFC 4240 [144] conference service; or
- RFC 6230 [146] and RFC 6505 [148].

### 10.3.3.2 Basic network media services with SIP

The MRFC may support control of basic conferencing by the use of RFC 4240 [144] and the conference service described in RFC 4240 [144] subclause 5.

The media control commands are received from the AS either directly over the Mr' interface or via the S-CSCF over the ISC and Mr interfaces.

The MRFC acts as the media server described in RFC 4240 [144].

### 10.3.3.3 Media control channel framework and packages

The MRFC may support control of conference mixing by the use of RFC 6505 [148] and RFC 6230 [146].

An MRFC may support control of floor controlled conferences (as specified in 3GPP TS 24.147 [8B]), via the use of RFC 6230 [146] together with appropriate packages. The packages, or extensions to existing packages using RFC 6230 [146] framework are not specified in this release.

An MRFC may support control of session-mode messaging conferences (as specified in 3GPP TS 24.247 [8F]), via the use of RFC 6230 [146] together with appropriate packages. The packages, or extensions to existing packages using RFC 6230 [146] framework are not specified in this release.

The MRFC shall send media control command responses and notifications to the AS using the AS-MRFC Cr interface.

The MRFC shall implement the control server role as described in RFC 6230 [146].

## 10.3.4 Transcoding

### 10.3.4.1 General

An MRFC may support control of transcoding. An MRFC supporting control of transcoding shall support one or more of the following methods:

- RFC 4240 [144] conference service;
- RFC 6230 [146] and RFC 6505 [148]; or
- RFC 4117 [166]. This is detailed in subclause 5.7.5.6.

### 10.3.4.2 Basic network media services with SIP

The MRFC may support control of transcoding by the use of RFC 4240 [144] and the conference service described in RFC 4240 [144] subclause 5.

The media control commands are received from the AS either directly over the Mr' interface or via the S-CSCF over the ISC and Mr interfaces.

The MRFC acts as the media server described in RFC 4240 [144].

### 10.3.4.3 Media control channel framework and packages

The MRFC may support control of transcoding by the use of RFC 6505 [148] and RFC 6230 [146].

The MRFC shall send media control command responses and notifications to the AS using the AS-MRFC Cr interface.

The MRFC shall implement the control server role as described in RFC 6230 [146].

## 10.4 Procedures at the MRB

The MRB shall support:

- a) the in-line unaware MRB interface.

as defined in RFC 6917 [192].

The MRB may support:

- a) the media server resource publish interface; and
- b) the media server resource consumer interface;

as defined in RFC 6917 [192].

---

# Annex A (normative): Profiles of IETF RFCs for 3GPP usage

## A.1 Profiles

### A.1.1 Relationship to other specifications

This annex contains a profile to the IETF specifications which are referenced by this specification, and the PICS proformas underlying profiles do not add requirements to the specifications they are proformas for.

This annex provides a profile specification according to both the current IETF specifications for SIP, SDP and other protocols (as indicated by the "RFC status" column in the tables in this annex) which are referenced by this specification and to the 3GPP specifications using SIP (as indicated by the "Profile status" column in the tables in this annex).

In the "RFC status" column the contents of the referenced specification takes precedence over the contents of the entry in the column.

In the "Profile status" column, there are a number of differences from the "RFC status" column. Where these differences occur, these differences take precedence over any requirements of the IETF specifications. Where specification concerning these requirements exists in the main body of the present document, the main body of the present document takes precedence.

Where differences occur in the "Profile status" column, the "Profile status" normally gives more strength to a "RFC status" and is not in contradiction with the "RFC status", e.g. it may change an optional "RFC status" to a mandatory "Profile status". If the "Profile status" weakens the strength of a "RFC status" then additionally this will be indicated by further textual description in the present document.

For all IETF specifications that are not referenced by this document or that are not mentioned within the 3GPP profile of SIP and SDP, the generic rules as defined by RFC 3261 [26] and in addition the rules in clauses 5 and 6 of this specification apply, e.g..

- a proxy which is built in accordance to this specification passes on any unknown method, unknown header field or unknown header field parameter after applying procedures such as filtering, insertion of P-Asserted-Identity header field, etc.;
- an UA which is built in accordance to this specification will
  - handle received unknown methods in accordance to the procedures defined in RFC 3261 [26], e.g. respond with a 501 (Not Implemented) response; and
  - handle unknown header fields and unknown header field parameters in accordance to the procedures defined in RFC 3261 [26], e.g. respond with a 420 (Bad Extension) if an extension identified by an option-tag in the Require header field of the received request is not supported by the UA.

### A.1.2 Introduction to methodology within this profile

This subclause does not reflect dynamic conformance requirements but static ones. In particular, a condition for support of a PDU parameter does not reflect requirements about the syntax of the PDU (i.e. the presence of a parameter) but the capability of the implementation to support the parameter.

In the sending direction, the support of a parameter means that the implementation is able to send this parameter (but it does not mean that the implementation always sends it).

In the receiving direction, it means that the implementation supports the whole semantic of the parameter that is described in the main part of this specification.

As a consequence, PDU parameter tables in this subclause are not the same as the tables describing the syntax of a PDU in the reference specification, e.g. RFC 3261 [26] tables 2 and 3. It is not rare to see a parameter which is optional in the syntax but mandatory in subclause below.

The various statii used in this subclause are in accordance with the rules in table A.1.

**Table A.1: Key to status codes**

| Status code | Status name           | Meaning  |
|-------------|-----------------------|--|
| m           | mandatory             | the capability shall be supported. It is a static view of the fact that the conformance requirements related to the capability in the reference specification are mandatory requirements. This does not mean that a given behaviour shall always be observed (this would be a dynamic view), but that it shall be observed when the implementation is placed in conditions where the conformance requirements from the reference specification compel it to do so. For instance, if the support for a parameter in a sent PDU is mandatory, it does not mean that it shall always be present, but that it shall be present according to the description of the behaviour in the reference specification (dynamic conformance requirement). |
| o           | optional              | the capability may or may not be supported. It is an implementation choice.  |
| n/a         | not applicable        | it is impossible to use the capability. No answer in the support column is required.   |
| x           | prohibited (excluded) | It is not allowed to use the capability. This is more common for a profile.  |
| c <integer> | conditional           | the requirement on the capability ("m", "o", "n/a" or "x") depends on the support of other optional or conditional items. <integer> is the identifier of the conditional expression.   |
| o.<integer> | qualified optional    | for mutually exclusive or selectable options from a set. <integer> is the identifier of the group of options, and the logic of selection of the options.   |
| i           | irrelevant            | capability outside the scope of the given specification. Normally, this notation should be used in a base specification ICS proforma only for transparent parameters in received PDUs. However, it may be useful in other cases, when the base specification is in fact based on another standard.   |

In the context of this specification the "i" status code mandates that the implementation does not change the content of the parameter. It is an implementation option if the implementation acts upon the content of the parameter (e.g. by setting filter criteria to known or unknown parts of parameters in order to find out the route a message has to take).

It must be understood, that this 3GPP SIP profile does not list all parameters which an implementation will treat as indicated by the status code "irrelevant". In general an implementation will pass on all unknown messages, header fields and header field parameters, as long as it can perform its normal behaviour.

The following additional comments apply to the interpretation of the tables in this Annex.

NOTE 1: The tables are constructed according to the conventional rules for ICS proformas and profile tables.

NOTE 2: The notation (either directly or as part of a conditional) of "m" for the sending of a parameter and "i" for the receipt of the same parameter, may be taken as indicating that the parameter is passed on transparently, i.e. without modification. Where a conditional applies, this behaviour only applies when the conditional is met.

As an example, the profile for the MGCF is found by first referring to clause 4.1, which states "The MGCF shall provide the UA role". Profiles are divided at the top level into the two roles in table A.2, user agent and proxy. The UA role is defined in subclause A.2.1 and the proxy role is defined in subclause A.2.2. More specific roles are listed in table A.3, table A.3A, table A.3B and table A.3C. The MGCF role is item 6 in table A.3 (the MGCF role is not found in table A.3A or table A.3B). Therefore, all profile entries for the MGCF are found by searching for A.3/6 in subclause A.2.1.

As a further example, to look up support of the Reason header field, table A.4 item 38 lists the Reason header field as a major capability that is optional for the user agent role. A subsequent search for A.4/38 in subclause A.2.1 shows that the Reason header field is optional for a user agent role to send and receive for ACK, BYE, CANCEL, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, PUBLISH, REFER, REGISTER, SUBSCRIBE, and UPDATE requests. Also, table A.162 item 48 lists the Reason header field as a major capability that is optional for the proxy role. A subsequent search for A.162/48 in subclause A.2.2 shows that, if supported, the Reason header field is mandatory to send and irrelevant to receive for ACK, BYE, CANCEL, INVITE, MESSAGE, NOTIFY, OPTIONS, PRACK, PUBLISH, REFER, REGISTER, SUBSCRIBE, and UPDATE requests.

## A.1.3 Roles

**Table A.2: Roles**

| Item  | Roles   | Reference | RFC status | Profile status |
|-------|---|-----------|------------|----------------|
| 1     | User agent  | [26]      | o.1        | o.1            |
| 2     | Proxy   | [26]      | o.1        | o.1            |
| o.1:  | It is mandatory to support exactly one of these items.  |           |            |                |
| NOTE: | For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role. |           |            |                |

Table A.3: Roles specific to this profile

| Item  | Roles   | Reference              | RFC status | Profile status |
|-------|---|------------------------|------------|----------------|
| 1     | UE  | 5.1                    | n/a        | o.1            |
| 1A    | UE containing UICC  | 5.1                    | n/a        | c5             |
| 1B    | UE without UICC   | 5.1                    | n/a        | c5             |
| 2     | P-CSCF  | 5.2                    | n/a        | o.1            |
| 2A    | P-CSCF (IMS-ALG)  | [7]                    | n/a        | c6             |
| 3     | I-CSCF  | 5.3                    | n/a        | o.1            |
| 3A    | void  |                        |            |                |
| 4     | S-CSCF  | 5.4                    | n/a        | o.1            |
| 5     | BGCF  | 5.6                    | n/a        | o.1            |
| 6     | MGCF  | 5.5                    | n/a        | o.1            |
| 7     | AS  | 5.7                    | n/a        | o.1            |
| 7A    | AS acting as terminating UA, or redirect server   | 5.7.2                  | n/a        | c2             |
| 7B    | AS acting as originating UA   | 5.7.3                  | n/a        | c2             |
| 7C    | AS acting as a SIP proxy  | 5.7.4                  | n/a        | c2             |
| 7D    | AS performing 3rd party call control  | 5.7.5                  | n/a        | c2             |
| 8     | MRFC  | 5.8                    | n/a        | o.1            |
| 8A    | MRB   | 5.8A                   | n/a        | o.1            |
| 9     | IBCF  | 5.10                   | n/a        | o.1            |
| 9A    | IBCF (THIG)   | 5.10.4                 | n/a        | c4             |
| 9B    | IBCF (IMS-ALG)  | 5.10.5, 5.10.7         | n/a        | c4             |
| 9C    | IBCF (Screening of SIP signalling)  | 5.10.6                 | n/a        | c4             |
| 9D    | IBCF (Privacy protection)   | 5.10.8                 | n/a        | c4             |
| 10    | Additional routeing functionality   | Annex I                | n/a        | c3             |
| 11    | E-CSCF  | 5.11                   | n/a        | o.1            |
| 11A   | E-CSCF acting as UA   | 5.11.1, 5.11.2, 5.11.3 | n/a        | c7             |
| 11B   | E-CSCF acting as a SIP Proxy  | 5.11.1, 5.11.2         | n/a        | c7             |
| 12    | LRF   | 5.12                   | n/a        | o.1            |
| 13    | ISC gateway function  | 5.13                   | n/a        | o.1            |
| 13A   | ISC gateway function (THIG)   | 5.13.4                 | n/a        | c8             |
| 13B   | ISC gateway function (IMS-ALG)  | 5.13.5                 | n/a        | c8             |
| 13C   | ISC gateway function (Screening of SIP signalling)  | 5.13.6                 | n/a        | c8             |
| c2:   | IF A.3/7 THEN o.2 ELSE n/a -- AS.   |                        |            |                |
| c3:   | IF A.3/3 OR A.3/4 OR A.3/5 OR A.3/6 OR A.3/9 THEN o ELSE o.1 -- I-CSCF, S-CSCF, BGCF, MGCF, IBCF.   |                        |            |                |
| c4:   | IF A.3/9 THEN o.3 ELSE n/a -- IBCF.   |                        |            |                |
| c5:   | IF A.3/1 THEN o.4 ELSE n/a -- UE.   |                        |            |                |
| c6:   | IF A.3/2 THEN o ELSE n/a -- P-CSCF.   |                        |            |                |
| c7:   | IF A.3/11 THEN o.5 ELSE n/a -- E-CSCF.  |                        |            |                |
| c8:   | IF A.3/13 THEN o ELSE n/a -- ISC gateway function.  |                        |            |                |
| o.1:  | It is mandatory to support exactly one of these items.  |                        |            |                |
| o.2:  | It is mandatory to support at least one of these items.   |                        |            |                |
| o.3:  | It is mandatory to support at least one of these items.   |                        |            |                |
| o.4:  | It is mandatory to support exactly one of these items.  |                        |            |                |
| o.5:  | It is mandatory to support exactly one of these items.  |                        |            |                |
| NOTE: | For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role. |                        |            |                |

**Table A.3A: Roles specific to additional capabilities**



| Item | Roles   | Reference               | RFC status | Profile status |
|------|---|-------------------------|------------|----------------|
| 1    | Presence server   | 3GPP TS 24.141<br>[8A]  | n/a        | c1             |
| 2    | Presence user agent                                       | 3GPP TS 24.141<br>[8A]  | n/a        | c2             |
| 3    | Resource list server                                      | 3GPP TS 24.141<br>[8A]  | n/a        | c3             |
| 4    | Watcher   | 3GPP TS 24.141<br>[8A]  | n/a        | c4             |
| 11   | Conference focus  | 3GPP TS 24.147<br>[8B]  | n/a        | c11            |
| 12   | Conference participant                                    | 3GPP TS 24.147<br>[8B]  | n/a        | c6             |
| 21   | CSI user agent  | 3GPP TS 24.279<br>[8E]  | n/a        | c7             |
| 22   | CSI application server                                    | 3GPP TS 24.279<br>[8E]  | n/a        | c8             |
| 31   | Messaging application server                              | 3GPP TS 24.247<br>[8F]  | n/a        | c5             |
| 32   | Messaging list server                                     | 3GPP TS 24.247<br>[8F]  | n/a        | c5             |
| 33   | Messaging participant                                     | 3GPP TS 24.247<br>[8F]  | n/a        | c2             |
| 33A  | Page-mode messaging participant                           | 3GPP TS 24.247<br>[8F]  | n/a        | c2             |
| 33B  | Session-mode messaging participant                        | 3GPP TS 24.247<br>[8F]  | n/a        | c2             |
| 34   | Session-mode messaging intermediate node                  | 3GPP TS 24.247<br>[8F]  | n/a        | c5             |
| 50   | Multimedia telephony service participant                  | 3GPP TS 24.173<br>[8H]  | n/a        | c2             |
| 50A  | Multimedia telephony service application server           | 3GPP TS 24.173<br>[8H]  | n/a        | c9             |
| 51   | Message waiting indication subscriber UA                  | 3GPP TS 24.606<br>[8I]  | n/a        | c2             |
| 52   | Message waiting indication notifier UA                    | 3GPP TS 24.606<br>[8I]  | n/a        | c3             |
| 53   | Advice of charge application server                       | 3GPP TS 24.647<br>[8N]  | n/a        | c8             |
| 54   | Advice of charge UA client                                | 3GPP TS 24.647<br>[8N]  | n/a        | c2             |
| 55   | Ut reference point XCAP server for supplementary services | 3GPP TS 24.623<br>[8P]  | n/a        | c3             |
| 56   | Ut reference point XCAP client for supplementary services | 3GPP TS 24.623<br>[8P]  | n/a        | c2             |
| 57   | Customized alerting tones application server              | 3GPP TS 24.182<br>[8Q]  | n/a        | c8             |
| 58   | Customized alerting tones UA client                       | 3GPP TS 24.182<br>[8Q]  | n/a        | c2             |
| 59   | Customized ringing signal application server              | 3GPP TS 24.183<br>[8R]  | n/a        | c8             |
| 60   | Customized ringing signal UA client                       | 3GPP TS 24.183<br>[8R]  | n/a        | c2             |
| 61   | SM-over-IP sender   | 3GPP TS 24.341<br>[8L]  | n/a        | c2             |
| 62   | SM-over-IP receiver                                       | 3GPP TS 24.341<br>[8L]  | n/a        | c2             |
| 63   | IP-SM-GW  | 3GPP TS 24.341<br>[8L]  | n/a        | c1             |
| 71   | IP-SM-GW  | 3GPP TS 29.311<br>[15A] | n/a        | c10            |
| 81   | MSC Server enhanced for ICS                               | 3GPP TS 24.292<br>[8O]  | n/a        | c12            |
| 82   | ICS user agent  | 3GPP TS 24.292<br>[8O]  | n/a        | c2             |
| 83   | SCC application server                                    | 3GPP TS 24.292<br>[8O]  | n/a        | c9             |

|         |   |                         |     |              |
|---------|---|-------------------------|-----|--------------|
| 84      | EATF  | 3GPP TS 24.237<br>[8M]  | n/a | c12          |
| 85      | In-dialog overlap signalling application server   | Annex N.2, Annex N.3.3  | n/a | c9           |
| 86      | In-dialog overlap signalling UA client  | Annex N.2, Annex N.3.3  | n/a | c2           |
| 87      | Session continuity controller UE  | 3GPP TS 24.337<br>[8ZC] | n/a | c2           |
| 88      | ATCF (proxy)  | 3GPP TS 24.237<br>[8M]  | n/a | c13 (note 4) |
| 89      | ATCF (UA)   | 3GPP TS 24.237<br>[8M]  | n/a | c12 (note 4) |
| 91      | Malicious communication identification application server   | 3GPP TS 24.616<br>[8S]  | n/a | c9           |
| 92      | USSI UE   | 3GPP TS 24.390<br>[8W]  | n/a | c2           |
| 93      | USSI AS   | 3GPP TS 24.390<br>[8W]  | n/a | c3           |
| c1:     | IF A.3/7A AND A.3/7B THEN o ELSE n/a - - AS acting as terminating UA, or redirect server and AS acting as originating UA.   |                         |     |              |
| c2:     | IF A.3/1 THEN o ELSE n/a - - UE.  |                         |     |              |
| c3:     | IF A.3/7A THEN o ELSE n/a - - AS acting as terminating UA, or redirect server.  |                         |     |              |
| c4:     | IF A.3/1 OR A.3/7B THEN o ELSE n/a - - UE or AS acting as originating UA.   |                         |     |              |
| c5:     | IF A.3/7D AND A.3/8 THEN o ELSE n/a - - AS performing 3rd party call control and MRFC (note 2).   |                         |     |              |
| c6:     | IF A.3/1 OR A.3A/11 THEN o ELSE n/a - - UE or conference focus.   |                         |     |              |
| c7:     | IF A.3/1 THEN o ELSE n/a - - UE.  |                         |     |              |
| c8:     | IF A.3/7D THEN o ELSE n/a - - AS performing 3rd party call control.   |                         |     |              |
| c9:     | IF A.3/7A OR A.3/7B OR A.3/7C OR A.3/7D THEN o ELSE n/a - - AS acting as terminating UA, or redirect server, AS acting as originating UA, AS acting as a SIP proxy, AS performing 3rd party call control.   |                         |     |              |
| c10:    | IF A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control.   |                         |     |              |
| c11:    | IF A.3/7D THEN o ELSE n/a - - AS performing 3rd party call control.   |                         |     |              |
| c12:    | IF A.2/1 THEN o ELSE n/a - - UA.  |                         |     |              |
| c13:    | IF A.2/2 THEN o ELSE n/a - - proxy.   |                         |     |              |
| NOTE 1: | For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role. |                         |     |              |
| NOTE 2: | The functional split between the MRFC and the AS for page-mode messaging is out of scope of this document and they are assumed to be collocated.  |                         |     |              |
| NOTE 3: | A.3A/63 is an AS providing the IP-SM-GW role to support the transport level interworking defined in 3GPP TS 24.341 [8L]. A.3A/71 is an AS providing the IP-SM-GW role to support the service level interworking for messaging as defined in 3GPP TS 29.311 [15A].                         |                         |     |              |
| NOTE 4: | An ATCF shall support both the ATCF (proxy) role and the ATCF (UA) role.  |                         |     |              |

Table A.3B: Roles with respect to access technology

| Item | Value used in P-Access-Network-Info header field        | Reference | RFC status | Profile status |
|------|---|-----------|------------|----------------|
| 1    | 3GPP-GERAN  | [52] 4.4  | o          | c1             |
| 2    | 3GPP-UTRAN-FDD  | [52] 4.4  | o          | c1             |
| 3    | 3GPP-UTRAN-TDD  | [52] 4.4  | o          | c1             |
| 4    | 3GPP2-1X  | [52] 4.4  | o          | c1             |
| 5    | 3GPP2-1X-HRPD   | [52] 4.4  | o          | c1             |
| 6    | 3GPP2-UMB   | [52] 4.4  | o          | c1             |
| 7    | 3GPP-E-UTRAN-FDD  | [52] 4.4  | o          | c1             |
| 8    | 3GPP-E-UTRAN-TDD  | [52] 4.4  | o          | c1             |
| 9    | 3GPP2-1X-Femto  | [52] 4.4  | o          | c1             |
| 11   | IEEE-802.11   | [52] 4.4  | o          | c1             |
| 12   | IEEE-802.11a  | [52] 4.4  | o          | c1             |
| 13   | IEEE-802.11b  | [52] 4.4  | o          | c1             |
| 14   | IEEE-802.11g  | [52] 4.4  | o          | c1             |
| 15   | IEEE-802.11n  | [52] 4.4  | o          | c1             |
| 21   | ADSL  | [52] 4.4  | o          | c1             |
| 22   | ADSL2   | [52] 4.4  | o          | c1             |
| 23   | ADSL2+  | [52] 4.4  | o          | c1             |
| 24   | RADSL   | [52] 4.4  | o          | c1             |
| 25   | SDSL  | [52] 4.4  | o          | c1             |
| 26   | HDSL  | [52] 4.4  | o          | c1             |
| 27   | HDSL2   | [52] 4.4  | o          | c1             |
| 28   | G.SHDSL   | [52] 4.4  | o          | c1             |
| 29   | VDSL  | [52] 4.4  | o          | c1             |
| 30   | IDSL  | [52] 4.4  | o          | c1             |
| 41   | DOCSIS  | [52] 4.4  | o          | c1             |
| 51   | DVB-RCS2  | [52] 4.4  | o          | c1             |
| c1:  | If A.3/1 OR A.3/2 THEN o.1 ELSE n/a - - UE or P-CSCF.   |           |            |                |
| o.1: | It is mandatory to support at least one of these items. |           |            |                |

Table A.3C: Modifying roles

| Item  | Roles   | Reference | RFC status | Profile status |
|-------|---|-----------|------------|----------------|
| 1     | UE performing the functions of an external attached network   | 4.1       |            |                |
| NOTE: | This table identifies areas where the behaviour is modified from that of the underlying role. Subclause 4.1 indicates which underlying roles are modified for this behaviour. |           |            |                |

Table A.3D: Roles with respect to security mechanism

| Item | Security mechanism  | Reference     | RFC status | Profile status |
|------|---|---------------|------------|----------------|
| 1    | IMS AKA plus IPsec ESP  | clause 4.2B.1 | n/a        | c1             |
| 2    | SIP digest plus check of IP association   | clause 4.2B.1 | n/a        | c2             |
| 3    | SIP digest plus Proxy Authentication  | clause 4.2B.1 | n/a        | c2             |
| 4    | SIP digest with TLS   | clause 4.2B.1 | n/a        | c2             |
| 5    | NASS-IMS bundled authentication   | clause 4.2B.1 | n/a        | c2             |
| 6    | GPRS-IMS-Bundled authentication   | clause 4.2B.1 | n/a        | c2             |
| 7    | Trusted node authentication   | clause 4.2B.1 | n/a        | c3             |
| 20   | End-to-end media security using SDES  | clause 4.2B.2 | o          | c5             |
| 21   | End-to-end media security using KMS   | clause 4.2B.2 | o          | c5             |
| 30   | End-to-access-edge media security using SDES  | clause 4.2B.2 | n/a        | c4             |
| c1:  | IF (A.3/1A OR A.3/2 OR A.3/3 OR A.3/4) THEN m ELSE IF A.3/1B THEN o ELSE n/a - - UE containing UICC or P-CSCF or I-CSCF or S-CSCF, UE without UICC. |               |            |                |
| c2:  | IF (A.3/1 OR A.3/2 OR A.3/3 OR A.3/4) THEN o ELSE n/a - - UE or P-CSCF or I-CSCF or S-CSCF.   |               |            |                |
| c3:  | IF (A.3/3 OR A.3/4) THEN o ELSE n/a - - I-CSCF or S-CSCF.   |               |            |                |
| c4:  | IF (A.3/1 OR A.3/2A) THEN o ELSE n/a - - UE or P-CSCF (IMS-ALG).  |               |            |                |
| c5:  | IF A.3/1 THEN o - - UE.   |               |            |                |

---

## A.2 Profile definition for the Session Initiation Protocol as used in the present document

### A.2.1 User agent role

#### A.2.1.1 Introduction

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for UA implementations:

Prerequisite: A.2/1 - - user agent role.

## A.2.1.2 Major capabilities

**Table A.4: Major capabilities**

| Item | Does the implementation support  | Reference              | RFC status | Profile status |
|------|--|------------------------|------------|----------------|
|      | <b>Capabilities within main protocol</b>   |                        |            |                |
| 1    | client behaviour for registration?   | [26] subclause 10.2    | o          | c3             |
| 2    | registrar?   | [26] subclause 10.3    | o          | c4             |
| 2A   | registration of multiple contacts for a single address of record   | [26] 10.2.1.2, 16.6    | o          | o              |
| 2B   | initiating a session?  | [26] subclause 13      | o          | o              |
| 2C   | initiating a session which require local and/or remote resource reservation?   | [30]                   | o          | c43            |
| 3    | client behaviour for INVITE requests?  | [26] subclause 13.2    | c18        | c18            |
| 4    | server behaviour for INVITE requests?  | [26] subclause 13.3    | c18        | c18            |
| 5    | session release?   | [26] subclause 15.1    | c18        | c18            |
| 6    | timestamping of requests?  | [26] subclause 8.2.6.1 | o          | o              |
| 7    | authentication between UA and UA?  | [26] subclause 22.2    | c34        | c34            |
| 8    | authentication between UA and registrar?   | [26] subclause 22.2    | o          | c74            |
| 8A   | authentication between UA and proxy?   | [26] 20.28, 22.3       | o          | c75            |
| 9    | server handling of merged requests due to forking?   | [26] 8.2.2.2           | m          | m              |
| 10   | client handling of multiple responses due to forking?  | [26] 13.2.2.4          | m          | m              |
| 11   | insertion of date in requests and responses?   | [26] subclause 20.17   | o          | o              |
| 12   | downloading of alerting information?   | [26] subclause 20.4    | o          | o              |
|      | <b>Extensions</b>  |                        |            |                |
| 13   | SIP INFO method and package framework?   | [25]                   | o          | c100           |
| 13A  | legacy INFO usage?   | [25] 2, 3              | o          | c90            |
| 14   | reliability of provisional responses in SIP?   | [27]                   | c19        | c44            |
| 15   | the REFER method?  | [36]                   | o          | c33            |
| 16   | integration of resource management and SIP?  | [30] [64]              | c19        | c44            |
| 17   | the SIP UPDATE method?   | [29]                   | c5         | c44            |
| 19   | SIP extensions for media authorization?  | [31]                   | o          | c14            |
| 20   | SIP specific event notification?   | [28]                   | o          | c13            |
| 21   | the use of NOTIFY to establish a dialog?   | [28] 4.2               | o          | n/a            |
| 22   | acting as the notifier of event information?   | [28]                   | c2         | c15            |
| 23   | acting as the subscriber to event information?   | [28]                   | c2         | c16            |
| 24   | session initiation protocol extension header field for registering non-adjacent contacts?  | [35]                   | o          | c6             |
| 25   | private extensions to the Session Initiation Protocol (SIP) for network asserted identity within trusted networks?   | [34]                   | o          | m              |
| 26   | a privacy mechanism for the Session Initiation Protocol (SIP)?   | [33]                   | o          | m              |
| 26A  | request of privacy by the inclusion of a Privacy header indicating any privacy option?   | [33]                   | c9         | c11            |
| 26B  | application of privacy based on the received Privacy header?   | [33]                   | c9         | n/a            |
| 26C  | passing on of the Privacy header transparently?  | [33]                   | c9         | c12            |
| 26D  | application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the assistance of intermediaries are obscured? | [33] 5.1               | c10        | c27            |

|     |  |                            |     |      |
|-----|--|----------------------------|-----|------|
| 26E | application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs? | [33] 5.2                   | c10 | c27  |
| 26F | application of the privacy option "user" such that user level privacy functions are provided by the network?             | [33] 5.3                   | c10 | c27  |
| 26G | application of the privacy option "id" such that privacy of the network asserted identity is provided by the network?    | [34] 7                     | c10 | n/a  |
| 26H | application of the privacy option "history" such that privacy of the History-Info header is provided by the network?     | [66] 7.2                   | c37 | c37  |
| 27  | a messaging mechanism for the Session Initiation Protocol (SIP)?   | [50]                       | o   | c7   |
| 28  | session initiation protocol extension header field for service route discovery during registration?                      | [38]                       | o   | c17  |
| 29  | compressing the session initiation protocol?   | [55]                       | o   | c8   |
| 30  | private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)?          | [52]                       | o   | m    |
| 30A | act as first entity within the trust domain for asserted identity?   | [34]                       | c96 | c97  |
| 30B | act as entity within trust network that can route outside the trust network?   | [34]                       | c96 | c97  |
| 30C | act as entity passing on identity transparently independent of trust domain?   | [34]                       | c96 | c98  |
| 31  | the P-Associated-URI header extension?   | [52] 4.1, [52A] 4          | c21 | c22  |
| 32  | the P-Called-Party-ID header extension?  | [52] 4.2, [52A] 4          | c21 | c23  |
| 33  | the P-Visited-Network-ID header extension?   | [52] 4.3, [52A] 4          | c21 | c24  |
| 34  | the P-Access-Network-Info header extension?  | [52] 4.4, [52A] 4, [234] 2 | c21 | c25  |
| 35  | the P-Charging-Function-Addresses header extension?  | [52] 4.5, [52A] 4          | c21 | c26  |
| 36  | the P-Charging-Vector header extension?  | [52] 4.6, [52A] 4          | c21 | c26  |
| 37  | security mechanism agreement for the session initiation protocol?  | [48]                       | o   | c20  |
| 37A | mediasec header field parameter for marking security mechanisms related to media?  | Subclause 7.2A.7           | n/a | c101 |
| 38  | the Reason header field for the session initiation protocol?   | [34A]                      | o   | c68  |
| 38A | carrying Q.850 codes in reason header fields in SIP (Session Initiation Protocol) responses?                             | [130]                      | o   | c82  |
| 39  | an extension to the session initiation protocol for symmetric response routing?  | [56A]                      | o   | c62  |
| 40  | caller preferences for the session initiation protocol?  | [56B]                      | C29 | c29  |
| 40A | the proxy-directive within caller-preferences?   | [56B] 9.1                  | o.5 | o.5  |
| 40B | the cancel-directive within caller-preferences?  | [56B] 9.1                  | o.5 | o.5  |
| 40C | the fork-directive within caller-preferences?  | [56B] 9.1                  | o.5 | o.5  |

|     |   |           |     |              |
|-----|---|-----------|-----|--------------|
| 40D | the recurse-directive within caller-preferences?  | [56B] 9.1 | o.5 | o.5          |
| 40E | the parallel-directive within caller-preferences?   | [56B] 9.1 | o.5 | o.5          |
| 40F | the queue-directive within caller-preferences?  | [56B] 9.1 | o.5 | o.5          |
| 41  | an event state publication extension to the session initiation protocol?  | [70]      | o   | c30          |
| 42  | SIP session timer?  | [58]      | c19 | c19          |
| 43  | the SIP Referred-By mechanism?  | [59]      | o   | c33          |
| 44  | the Session Initiation Protocol (SIP) "Replaces" header?  | [60]      | c19 | c38 (note 1) |
| 45  | the Session Initiation Protocol (SIP) "Join" header?  | [61]      | c19 | c19 (note 1) |
| 46  | the callee capabilities?  | [62]      | o   | c35          |
| 47  | an extension to the session initiation protocol for request history information?  | [66]      | o   | o            |
| 48  | Rejecting anonymous requests in the session initiation protocol?  | [67]      | o   | o            |
| 49  | session initiation protocol URIs for applications such as voicemail and interactive voice response?                             | [68]      | o   | o            |
| 50  | Session Initiation Protocol's (SIP) non-INVITE transactions?  | [84]      | m   | m            |
| 51  | the P-User-Database private header extension?   | [82] 4    | o   | c94          |
| 52  | a uniform resource name for services?   | [69]      | n/a | c39          |
| 53  | obtaining and using GRUUs in the Session Initiation Protocol (SIP)  | [93]      | o   | c40 (note 2) |
|     |   |           |     |              |
| 55  | the Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)?                       | [96]      | o   | c42          |
| 56  | the SIP P-Profile-Key private header extension?   | [97]      | n/a | n/a          |
| 57  | managing client initiated connections in SIP?   | [92]      | o   | c45          |
| 58  | indicating support for interactive connectivity establishment in SIP?   | [102]     | o   | c46          |
| 59  | multiple-recipient MESSAGE requests in the session initiation protocol?   | [104]     | c47 | c48          |
| 60  | SIP location conveyance?  | [89]      | o   | c49          |
| 61  | referring to multiple resources in the session initiation protocol?   | [105]     | c50 | c50          |
| 62  | conference establishment using request-contained lists in the session initiation protocol?                                      | [106]     | c51 | c52          |
| 63  | subscriptions to request-contained resource lists in the session initiation protocol?   | [107]     | c53 | c53          |
| 64  | dialstring parameter for the session initiation protocol uniform resource identifier?   | [103]     | o   | c19          |
| 65  | the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular? | [111]     | o   | c60          |
| 66  | the SIP P-Early-Media private header extension for authorization of early media?  | [109] 8   | o   | c58          |
| 67  | number portability parameters for the 'tel' URI?  | [112]     | o   | c54          |
| 67A | assert or process carrier indication?   | [112]     | o   | c55          |
| 67B | local number portability?   | [112]     | o   | c57          |
|     |   |           |     |              |
| 69  | extending the session initiation protocol Reason header for preemption events   | [115]     | c69 | c69          |



|     |   |                   |      |      |
|-----|---|-------------------|------|------|
| 70  | communications resource priority for the session initiation protocol?   | [116]             | o    | c70  |
| 70A | inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol?        | [116] 4.2         | c72  | c72  |
| 70B | inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol? | [116] 4.2         | c72  | c72  |
| 71  | addressing an amplification vulnerability in session initiation protocol forking proxies?                               | [117]             | o    | c87  |
| 72  | the remote application identification of applying signalling compression to SIP   | [79] 9.1          | o    | c8   |
| 73  | a session initiation protocol media feature tag for MIME application subtypes?  | [120]             | o    | c59  |
| 74  | SIP extension for the identification of services?   | [121]             | o    | c61  |
| 75  | a framework for consent-based communications in SIP?  | [125]             | c76  | c76  |
| 75A | a relay within the framework for consent-based communications in SIP?   | [125]             | c77  | c78  |
| 75B | a recipient within the framework for consent-based communications in SIP?   | [125]             | c80  | c79  |
| 76  | a mechanism for transporting user-to-user call control information in SIP?  | [126]             | o    | c81  |
| 76A | interworking ISDN call control user information with SIP?   | [126A]            | c109 | c109 |
| 77  | The SIP P-Private-Network-Indication private-header (P-Header)?   | [134]             | o    | o    |
| 78  | the SIP P-Served-User private header for the 3GPP IM CN subsystem?  | [133] 6           | o    | c93  |
| 79  | the SIP P-Served-User header extension for Originating CDIV session case?   | [239] 4           | c126 | c127 |
| 81  | the 199 (Early Dialog Terminated) response code)  | [142]             | o    | c86  |
| 82  | message body handling in SIP?   | [150]             | m    | m    |
| 83  | indication of support for keep-alive  | [143]             | o    | c88  |
| 84  | SIP Interface to VoiceXML Media Services?   | [145]             | o    | c89  |
| 85  | common presence and instant messaging (CPIM): message format?   | [151]             | o    | c91  |
| 86  | instant message disposition notification?   | [157]             | o    | c91  |
| 87  | requesting answering modes for SIP?   | [158]             | o    | c60  |
| 89  | the early session disposition type for SIP?   | [74B]             | o    | o    |
| 90  | delivery of Request-URI targets to user agents?   | Subclause 7.2A.16 | o    | c95  |
| 91  | The Session-ID header?  | [162]             | o    | c102 |
| 92  | correct transaction handling for 2xx responses to Session Initiation Protocol INVITE requests?                          | [163]             | c18  | c18  |
| 93  | addressing Record-Route issues in the Session Initiation Protocol (SIP)?  | [164]             | n/a  | n/a  |
| 94  | essential correction for IPv6 ABNF and URI comparison in RFC3261?   | [165]             | m    | m    |
| 95  | suppression of session initiation protocol REFER method implicit subscription?  | [173]             | o    | c99  |
| 96  | Alert-Info URNs for the Session Initiation Protocol?  | [175]             | o    | o    |
| 97  | multiple registrations?   | Subclause 3.1     | n/a  | c103 |

|      |   |   |      |      |
|------|---|---|------|------|
| 98   | the SIP P-Refused-URI-List private-header?  | [183]   | o    | c104 |
| 99   | request authorization through dialog Identification in the session initiation protocol? | [184]   | o    | c105 |
| 100  | indication of features supported by proxy?  | [190]   | o    | c106 |
| 101  | registration of bulk number contacts?   | [191]   | o    | c107 |
| 102  | media control channel framework?  | [146]   | o    | c108 |
| 103  | S-CSCF restoration procedures?  | Subclause 3.1                                       | n/a  | c110 |
| 104  | SIP overload control?   | [198]   | o    | c112 |
| 104A | feedback control?   | [199]   | c113 | c113 |
| 104B | distribution of load filters?   | [201]   | c113 | c114 |
| 105  | handling of a 380 (Alternative service) response?                                       | Subclauses 5.1.2A.1.1, 5.1.3.1, 5.1.6.8, and 5.2.10 | n/a  | c111 |

|      |  |
|------|--|
| c2:  | IF A.4/20 THEN o.1 ELSE n/a - - SIP specific event notification extension.   |
| c3:  | IF A.3/1 OR A.3/4 OR A.3A/81 THEN m ELSE n/a - - UE or S-CSCF functional entity or MSC Server enhanced for ICS.  |
| c4:  | IF A.3/4 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - S-CSCF or AS functional entity.  |
| c5:  | IF A.4/16 THEN m ELSE o - - integration of resource management and SIP extension.  |
| c6:  | IF A.3/4 OR A.3/1 OR A.3A/81 THEN m ELSE n/a. - - S-CSCF or UE or MSC Server enhanced for ICS.   |
| c7:  | IF A.3/1 OR A.3/4 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9B OR A.3/13B OR A.3A/83 OR A.3A/89 THEN m ELSE n/a - - UA or S-CSCF or AS acting as terminating UA or AS acting as originating UA or AS performing 3 <sup>rd</sup> party call control or IBCF (IMS-ALG), ISC gateway function (IMS-ALG), SCC application server, ATCF (UA).  |
| c8:  | IF A.3/1 THEN (IF (A.3B/1 OR A.3B/2 OR A.3B/3 OR A.3B/4 OR A.3B/5 OR A.3B/6 OR A.3B/7 OR A.3B/8 OR A.3B/11 OR A.3B/12 OR A.3B/13 OR A.3B/14 OR A.3B/15) THEN m ELSE o) ELSE n/a - - UE behaviour (based on P-Access-Network-Info usage).   |
| c9:  | IF A.4/26 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |
| c10: | IF A.4/26B THEN o.3 ELSE n/a - - application of privacy based on the received Privacy header.  |
| c11: | IF A.3/1 OR A.3/6 OR A.3A/81 THEN o ELSE IF A.3/9B OR A.3/13B THEN m ELSE n/a - - UE or MGCF, IBCF (IMS-ALG), ISC gateway function (IMS-ALG), MSC Server enhanced for ICS.   |
| c12: | IF A.3/7D OR A3A/84 OR A.3A/89 THEN m ELSE n/a - - AS performing 3 <sup>rd</sup> -party call control, EATF, ATCF (UA).   |
| c13: | IF A.3/1 OR A.3/2 OR A.3/4 OR A.3/9B OR A.3/11 OR A.3/12 OR A.3/13B OR A.3A/81 THEN m ELSE o - - UE or S-CSCF or IBCF (IMS-ALG) or E-CSCF or LRF or ISC gateway function (IMS-ALG) or MSC Server enhanced for ICS.   |
| c14: | IF A.3/1 AND A4/2B AND (A.3B/1 OR A.3B/2 OR A.3B/3) THEN m ELSE IF A.3/2 THEN o ELSE n/a - UE and initiating sessions and GPRS IP-CAN or P-CSCF.   |
| c15: | IF A.4/20 AND (A.3/4 OR A.3/9B OR A.3/11 OR A.3/13B) THEN m ELSE o - SIP specific event notification extensions and S-CSCF or IBCF (IMS-ALG) or E-CSCF or ISC gateway function (IMS-ALG).  |
| c16: | IF A.4/20 AND (A.3/1 OR A.3/2 OR A.3/9B OR A.3/12 OR A.3/13B OR A.3A/81) THEN m ELSE o - - SIP specific event notification extension and UE or P-CSCF or IBCF (IMS-ALG) or MSC Server enhanced for ICS or LRF or ISC gateway function (IMS-ALG).   |
| c17: | IF A.3/1 OR A.3/4 OR A.3A/81 THEN m ELSE n/a - - UE or S-CSCF or MSC Server enhanced for ICS.  |
| c18: | IF A.4/2B THEN m ELSE n/a - - initiating sessions.   |
| c19: | IF A.4/2B THEN o ELSE n/a - - initiating sessions.   |
| c20: | IF A.3/1 AND (A.3D/1 OR A.3D/4) THEN m ELSE n/a - - UE and (IMS AKA plus IPsec ESP or SIP digest with TLS).  |
| c21: | IF A.4/30 THEN o.4 ELSE n/a - - private header extensions to the session initiation protocol for the 3 <sup>rd</sup> -Generation Partnership Project (3GPP).   |
| c22: | IF A.4/30 AND (A.3/1 OR A.3/4 OR A.3A/81) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3 <sup>rd</sup> -Generation Partnership Project (3GPP) and S-CSCF or UE or MSC Server enhanced for ICS.   |
| c23: | IF A.4/30 AND (A.3/1 OR A.3A/81) THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3 <sup>rd</sup> -Generation Partnership Project (3GPP) and UE or MSC Server enhanced for ICS.  |
| c24: | IF A.4/30 AND (A.3/4 OR A.3A/81) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3 <sup>rd</sup> -Generation Partnership Project (3GPP) and S-CSCF or MSC Server enhanced for ICS.  |
| c25: | IF A.4/30 AND (A.3A/81 OR A.3/4 OR A.3/6 OR A.3/7A OR A.3/7D OR A.3/9B OR A.3/13B OR A3A/84) THEN m ELSE IF A.4/30 AND A.3/1 AND (A.3B/1 OR A.3B/2 OR A.3B/3 OR A.3B/4 OR A.3B/5 OR A.3B/6 OR A.3A/7 OR A.3A/8 OR A.3B/11 OR A.3B/12 OR A.3B/13 OR A.3B/14 OR A.3A/15 OR A.3B/41) THEN m ELSE IF A4/30 AND A.3/1 AND (A.3B/21 OR A.3B/22 OR A.3B/23 OR A.3B/24 OR A.3B/25 OR A.3B/26 OR A.3A/27 OR A.3A/28 OR A.3B/29 OR A.3B/30) THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3 <sup>rd</sup> -Generation Partnership Project (3GPP), MSC Server enhanced for ICS, S-CSCF, MGCF or AS acting as terminating UA or AS acting as third-party call controller or IBCF (IMS-ALG), ISC gateway function (IMS-ALG), UE, EATF, P-Access-Network-Info values. |
| c26: | IF A.4/30 AND (A.3A/81 OR (A.3/4 AND A.4/2) OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9B OR A.3/13B OR A3A/84 OR A.3A/89) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3 <sup>rd</sup> -Generation Partnership Project (3GPP) MSC Server enhanced for ICS, S-CSCF, registrar, MGCF, AS acting as a terminating UA, or AS acting as an originating UA, or AS acting as third-party call controller, IBCF (IMS-ALG), ISC gateway function (IMS-ALG), EATF, ATCF (UA).  |
| c27: | IF A.3/7D OR A.3/9D THEN o ELSE x - - AS performing 3 <sup>rd</sup> party call control, IBCF (Privacy).  |
| c29: | IF A.4/40A OR A.4/40B OR A.4/40C OR A.4/40D OR A.4/40E OR A.4/40F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol.   |
| c30: | IF A.3A/1 OR A.3A/2 THEN m ELSE IF A.3/1 THEN o ELSE n/a - - presence server, presence user agent, UE, AS.   |

|      |   |
|------|---|
| c33: | IF A.3/9B OR A.3/12 OR A.3/13B OR A.3A/81 OR A.3A/11 OR A.3A/12 OR A.4/44 THEN m ELSE o - - IBCF (IMS-ALG) or LRF or ISC gateway function (IMS-ALG) or MSC Server enhanced for ICS or conference focus or conference participant or the Session Initiation Protocol (SIP) "Replaces" header.  |
| c34: | IF A.4/44 OR A.4/45 OR A.3/9B OR A.3/13 THEN m ELSE n/a - - the Session Initiation Protocol (SIP) "Replaces" header or the Session Initiation Protocol (SIP) "Join" header or IBCF (IMS-ALG) or ISC gateway function (IMS-ALG).   |
| c35: | IF A.3/4 OR A.3/9B OR A.3/13B OR A.3A/82 OR A.3A/83 OR A.3A/21 OR A.3A/22 OR A3A/84 THEN m ELSE IF (A.3/1 OR A.3/6 OR A.3/7 OR A.3/8 OR A.3A/81) THEN o ELSE n/a - - S-CSCF or IBCF (IMS-ALG) or ISC gateway function (IMS-ALG) functional entities or ICS user agent or SCC application server or CSI user agent or CSI application server, UE or MGCF or AS or MRFC functional entity or MSC Server enhanced for ICS or EATF. |
| c37  | IF A.4/47 THEN o.3 ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c38: | IF A.4/2B AND (A.3A/11 OR A.3A/12 OR A.3/7D) THEN m ELSE IF A.4/2B THEN o ELSE n/a - - initiating sessions, conference focus, conference participant, AS performing 3rd party call control.   |
| c39: | IF A.3/1 THEN m ELSE IF A.3/7B OR A.3/7D OR A.3/9 THEN o ELSE n/a - - UE, AS acting as an originating UA, or AS acting as third-party call controller, IBCF.  |
| c40  | IF A.3/4 OR (A.3/1 AND NOT A.3C/1) OR A.3A/81 THEN m ELSE IF (A.3/7A OR A.3/7B OR A.3/7D) THEN o ELSE n/a - - S-CSCF, UE, UE performing the functions of an external attached network, MSC Server enhanced for ICS, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control.   |
| c42: | IF A.3/1 THEN n/a ELSE o - - UE.  |
| c43: | IF A.4/2B THEN o ELSE n/a - - initiating sessions.  |
| c44: | IF A.4/2C THEN m ELSE o - - initiating a session which require local and/or remote resource reservation.  |
| c45: | IF A.4/97 THEN m ELSE n/a - - multiple registrations.   |
| c46  | IF A.3/1 OR A.3/4 THEN o ELSE n/a - - UE, S-CSCF.   |
| c47: | IF A.4/27 THEN o ELSE n/a - - a messaging mechanism for the Session Initiation Protocol (SIP).  |
| c48: | IF A.3A/32 AND A.4/27 THEN m ELSE IF A.4/27 THEN o ELSE n/a - - messaging list server, a messaging mechanism for the Session Initiation Protocol (SIP).   |
| c49: | IF A.3/1 OR A.3/9B OR A.3/13B OR A.3A/81 OR A.3/11 OR A.3/12 OR A3A/84 THEN m ELSE o - - UE, IBCF (IMS-ALG), ISC gateway function (IMS-ALG), MSC Server enhanced for ICS, E-CSCF, LRF, EATF.  |
| c50: | IF A.3A/81 THEN n/a ELSE IF A.4/15 THEN o ELSE n/a - - MSC Server enhanced for ICS, the REFER method.   |
| c51: | IF A.4/2B THEN o ELSE n/a - - initiating a session.   |
| c52: | IF A.3A/11 AND A.4/2B THEN m ELSE IF A.4/2B THEN o ELSE n/a - - conference focus, initiating a session.   |
| c53: | IF A.3A/81 THEN n/a ELSE IF A.4/20 THEN o ELSE n/a - - MSC Server enhanced for ICS, SIP specific event notification.  |
| c54: | IF A.3/1 OR A.3/6 OR A.3/7A OR A.3/7D OR A.3/9 THEN o, ELSE n/a - - UE, MGCF, AS acting as originating UA, AS performing 3rd party call control, IBCF.  |
| c55: | IF A.4/67 THEN m ELSE n/a - - number portability parameters for the 'tel' URI.  |
| c57: | IF A.4/67 THEN m ELSE n/a - - number portability parameters for the 'tel' URI.  |
| c58: | IF A.3/9B OR A.3/13B OR A.3/6 OR A.3A/81 THEN m ELSE o - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), MGCF, MSC Server enhanced for ICS.   |
| c59: | IF A.3/4 THEN m ELSE IF (A.3/1 OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/8) THEN o ELSE n/a - - S-CSCF, UE, MGCF, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, or MRFC.  |
| c60: | IF A.3/9B OR A.3/13B THEN m ELSE IF A.3/1 OR A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), UE, AS acting as terminating UA, AS acting as originating UA, AS performing 3 <sup>rd</sup> party call control.   |
| c61: | IF (A.3/1 OR A.3A/81 OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/8 OR A.3/9B OR A.3/13 OR A3A/84) THEN o ELSE n/a - - UE, MSC Server enhanced for ICS, MGCF, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, or MRFC or IBCF (IMS-ALG), ISC gateway function (IMS-ALG), EATF.   |
| c62: | IF A.3/1 THEN o ELSE n/a - - UE.  |
| c68: | IF A.4/69 OR A.3A/83 THEN m ELSE o - - extending the session initiation protocol Reason header for preemption events and Q.850 causes, SCC application server.  |
| c69: | IF A.4/70 THEN o ELSE n/a - - communications resource priority for the session initiation protocol.   |
| c70: | IF A.3/9B OR A.3/13B THEN m ELSE IF A.3/1 OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3A/81 THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), UE, MGCF, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, MSC Server enhance for ICS.   |
| c72: | IF A.4/70 THEN o ELSE n/a - - communications resource priority for the session initiation protocol  |

|       |  |
|-------|--|
| c74:  | IF A.3/4 OR A.3/1 THEN o ELSE n/a. - - S-CSCF or UE.   |
| c75:  | IF A.3/1 THEN o ELSE n/a. - - UE.  |
| c76:  | IF A.4/75A OR A.4/75B THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP, a recipient within the framework for consent-based communications in SIP.  |
| c77:  | IF A.4/59 OR A.4/61 OR A.4/62 OR A.4/63 THEN m ELSE o - - multiple-recipient MESSAGE requests in the session initiation protocol, referring to multiple resources in the session initiation protocol, conference establishment using request-contained lists in the session initiation protocol, subscriptions to request-contained resource lists in the session initiation protocol.   |
| c78:  | IF (A.4/59 OR A.4/61 OR A.4/62 OR A.4/63) AND (A.3A/11 OR A.3A/31) THEN m ELSE o - - multiple-recipient MESSAGE requests in the session initiation protocol, referring to multiple resources in the session initiation protocol, conference establishment using request-contained lists in the session initiation protocol, subscriptions to request-contained resource lists in the session initiation protocol, conference focus, messaging application server.                          |
| c79:  | IF A.3/9B OR A.3/13B OR (A.3/1 AND (A.4/2B OR A.4/15 OR A.4/20 OR A.4/27)) THEN m ELSE IF A.3/6 OR A.3/7A OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), UE, initiating a session, the REFER method, SIP specific event notification, a messaging mechanism for the Session Initiation Protocol (SIP), AS acting as terminating UA, or redirect server, AS performing 3rd party call control.   |
| c80:  | IF A.4/2B OR A.4/15 OR A.4/20 OR A.4/27 THEN m ELSE n/a - - initiating a session, the REFER method, SIP specific event notification, a messaging mechanism for the Session Initiation Protocol (SIP).  |
| c81:  | IF A.3/1 OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE IF A.3/9B OR A.3/13B THEN m ELSE n/a - - UE, MGCF, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, IBCF (IMS-ALG), ISC gateway function (IMS-ALG).   |
| c82:  | IF A.3/6 THEN m ELSE n/a - - MGCF.   |
| c85:  | IF A.3/1 OR A.3A/81 OR A.3/2 OR A.3/7B THEN m ELSE n/a - - UE, MSC Server enhanced for ICS, P-CSCF, AS acting as originating UA.   |
| c86:  | IF A.4/3 OR A.4/4 THEN m ELSE n/a - - client behaviour for INVITE requests, server behaviour for INVITE requests.  |
| c87:  | IF A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C THEN m ELSE o - - IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling).  |
| c88:  | IF A.3/1 OR A.3/2 THEN m ELSE o - - UE, P-CSCF.  |
| c89:  | IF A.3/7A OR A.3/8 THEN o ELSE n/a - - AS performing 3rd party call control, MRFC.   |
| c90:  | IF A.4/13 OR A.3A/53 OR A.3A/54 OR A.3A/91 OR A.3A/85 OR A.3A/86 THEN m ELSE o - - SIP INFO method and package framework, advice of charge application server, advice of charge UA client, malicious communication identification application server, in-dialog overlap signalling application server, in-dialog overlap signalling UA client.   |
| c91:  | IF A.3A/61 OR A.3A/62 OR A.3A/63 OR A.3A/71 THEN m ELSE o - - SM-over-IP sender, SM-over-IP receiver, IP-SM-GW, IP-SM-GW.  |
| c93:  | IF A.3/7B OR A.3/7D OR A.3A/84 THEN o ELSE n/a - - AS acting as originating UA, AS performing 3rd party call control, EATF.  |
| c94:  | IF A.3/4 OR A.3/7A OR A.3/7D THEN o ELSE n/a - - S-CSCF and AS acting as terminating UA or redirect server or AS performing 3rd party call control.  |
| c95:  | IF A.3/7 THEN o ELSE n/a - - AS.   |
| c96:  | IF A.4/30 THEN o ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.   |
| c97:  | IF (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) AND A.4/30 THEN m ELSE IF (A.3/7D OR A.3/11 OR A.3C/1) AND A.4/30 THEN o ELSE n/a - - IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), AS performing 3rd party call control, E-CSCF, UE performing the functions of an external attached network and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks. |
| c98:  | IF A.3/7D OR A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C OR A.3C/1 OR A.3A/84 OR A.3A/89 THEN m ELSE n/a - - AS performing 3rd party call control, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE performing the functions of an external attached network, EATF, ATCF (UA).  |
| c99:  | IF A.4/15 AND (A.3/9B OR A.3/9C OR A.13/B OR A.13/C) THEN m ELSE IF A.4/15 THEN o ELSE n/a - - the REFER method, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling).   |
| c100: | IF A.3/6 OR A.3A/57 OR A.3A/58 OR A.3A/59 OR A.3A/60 THEN m ELSE o - - MGCF, customized alerting tones application server, customized alerting tones UA client, customized ringing signal application server, customized ringing signal UA client.   |
| c101: | IF A.3D/30 THEN m ELSE n/a - - end-to-access-edge media security using SDES.   |
| c102: | IF A.3A/11 OR A.3A/12 OR A.3/9 THEN m ELSE n/a - - conference focus, conference participant, IBCF.   |
| c103: | IF A.3/1 THEN o ELSE IF A.3/2 OR A.3/4 THEN m ELSE n/a - - UE, P-CSCF, S-CSCF.   |
| c104: | IF A.3/9B OR A.3/13B THEN m ELSE IF A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), AS acting as terminating UA, AS acting as originating UA, AS performing 3rd party call control.   |

|         |   |
|---------|---|
| c105:   | IF A.3/9B OR A.3/13B OR A.3A/82 OR A.3A/83 OR A.3A/87 OR A.3A/89 THEN m ELSE o - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), ICS user agent, SCC application server, Session continuity controller UE, ATCF (UA).   |
| c106:   | IF A.3A/50A OR A.3A/83 OR A.3A/89 THEN m ELSE o - - Multimedia telephony application server, SCC application server, ATCF (UA).   |
| c107:   | IF A.3C/1 OR A.4/2 THEN o ELSE n/a - - UE performing the functions of an external attached network, registrar.  |
| c108:   | IF A.3/7 OR A.3/8 OR A.3/8A THEN o ELSE n/a - - AS, MRFC, MRB.  |
| c109:   | IF A.4/76 THEN o ELSE n/a - - a mechanism for transporting user to user call control information in SIP.  |
| c110:   | IF A.3/1 THEN m ELSE IF A.3/2 OR A.3/3 OR A.3/4 THEN o ELSE n/a - - UE, P-CSCF, I-CSCF, S-CSCF.   |
| c111:   | IF A.3/1 OR A.3/2 THEN m ELSE n/a - - UE, P-CSCF.   |
| c112:   | IF NOT (A.3/1 AND NOT A.3C/1) THEN o ELSE n/a - - not UE, UE performing the functions of an external attached network.  |
| c113:   | IF A.4/104 THEN o.7 ELSE n/a - - SIP overload control.  |
| c114:   | IF A.4/104 THEN IF A.3/4 OR A.3/7 OR A.3/10 THEN o.7 ELSE n/a - - SIP overload control, S-CSCF, AS, additional routing functionality.   |
| c126:   | IF A.4/78 THEN o ELSE n/a - - the SIP P-Served-User private header for the 3GPP IM CN subsystem.  |
| c126:   | IF A.4/78 THEN m ELSE n/a - - the SIP P-Served-User private header for the 3GPP IM CN subsystem.  |
| o.1:    | At least one of these capabilities is supported.  |
| o.2:    | At least one of these capabilities is supported.  |
| o.3:    | At least one of these capabilities is supported.  |
| o.4:    | At least one of these capabilities is supported.  |
| o.5:    | At least one of these capabilities is supported.  |
| o.6:    | It is mandatory to support at least one of these items.   |
| o.7:    | At least one of these capabilities is supported.  |
| NOTE 1: | An AS acting as a proxy may be outside the trust domain, and therefore not able to support the capability for that reason; in this case it is perfectly reasonable for the header to be passed on transparently, as specified in the PDU parts of the profile.  |
| NOTE 2: | If a UE is unable to become engaged in a service that potentially requires the ability to identify and interact with a specific UE even when multiple UEs share the same single Public User Identity then the UE support can be "o" instead of "m". Examples include telemetry applications, where point-to-point communication is desired between two users. |

Prerequisite A.4/20 - - SIP specific event notification

**Table A.4A: Supported event packages**

| Item | Does the implementation support  | Subscriber   |            |                | Notifier     |            |                |
|------|--|--------------|------------|----------------|--------------|------------|----------------|
|      |  | Ref.         | RFC status | Profile status | Ref.         | RFC status | Profile status |
| 1    | reg event package?   | [43]         | c1         | c3             | [43]         | c2         | c4             |
| 1A   | reg event package extension for GRUUs?   | [94]         | c1         | c25            | [94]         | c2         | c4             |
| 2    | refer package?   | [36] 3       | c13        | c13            | [36] 3       | c13        | c13            |
| 3    | presence package?  | [74] 6       | c1         | c5             | [74] 6       | c2         | c6             |
| 4    | eventlist with underlying presence package?  | [75], [74] 6 | c1         | c7             | [75], [74] 6 | c2         | c8             |
| 5    | presence.wininfo template-package?   | [72] 4       | c1         | c9             | [72] 4       | c2         | c10            |
| 6    | xcap-diff package?   | [77] 4       | c1         | c11            | [77] 4       | c2         | c12            |
| 7    | conference package?  | [78] 3       | c1         | c21            | [78] 3       | c1         | c22            |
| 8    | message-summary package?   | [65]         | c1         | c23            | [65] 3       | c2         | c24            |
| 9    | poc-settings package?  | [110]        | c1         | c26            | [110]        | c2         | c27            |
| 11   | dialog event package?  | [171]        | c1         | c14            | [171]        | c2         | c15            |
| 12   | load-control package?  | [201]        | c29        | c30            | [201]        | c29        | c31            |
| c1:  | IF A.4/23 THEN o ELSE n/a - - acting as the subscriber to event information.   |              |            |                |              |            |                |
| c2:  | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.   |              |            |                |              |            |                |
| c3:  | IF A.3/1 OR A.3A/81 OR A.3/2 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - UE, MSC Server enhanced for ICS, P-CSCF, AS.   |              |            |                |              |            |                |
| c4:  | IF A.3/4 THEN m ELSE IF A.3C/1 THEN o ELSE n/a - - S-CSCF, UE performing the functions of an external attached network.  |              |            |                |              |            |                |
| c5:  | IF A.3A/3 OR A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - resource list server or watcher, acting as the subscriber to event information.  |              |            |                |              |            |                |
| c6:  | IF A.3A/1 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server, acting as the notifier of event information.  |              |            |                |              |            |                |
| c7:  | IF A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - watcher, acting as the subscriber to event information.  |              |            |                |              |            |                |
| c8:  | IF A.3A/3 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - resource list server, acting as the notifier of event information.   |              |            |                |              |            |                |
| c9:  | IF A.3A/2 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - presence user agent, acting as the subscriber to event information.  |              |            |                |              |            |                |
| c10: | IF A.3A/1 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server, acting as the notifier of event information.  |              |            |                |              |            |                |
| c11: | IF A.3A/2 OR A.3A/4 OR A.3A/56 THEN o ELSE IF A.4/23 THEN o ELSE n/a - - presence user agent or watcher or Ut reference point XCAP client for supplementary services, acting as the subscriber to event information.                                 |              |            |                |              |            |                |
| c12: | IF A.3A/1 OR A.3A/3 OR A.3A/55 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server or resource list server or Ut reference point XCAP server for supplementary services, acting as the notifier of event information.                          |              |            |                |              |            |                |
| c13: | IF A.4/15 THEN m ELSE n/a - - the REFER method.  |              |            |                |              |            |                |
| c14: | IF A.3/12 OR A.3A/87 THEN m ELSE IF A.3/1 OR A.3/7B OR A.3/7D THEN o ELSE n/a - - LRF, session continuity controller UE, UE, AS acting as originating UA, AS performing 3rd party call control.  |              |            |                |              |            |                |
| c15: | IF A.3/11 OR A.3A/83 THEN m ELSE IF A.3/1 OR A.3/7A OR A.3/7D THEN o ELSE n/a - - E-CSCF, SCC application server, UE, AS acting as terminating UA, or redirect server, AS performing 3rd party call control.   |              |            |                |              |            |                |
| c21: | IF A.3A/12 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - conference participant or acting as the subscriber to event information.  |              |            |                |              |            |                |
| c22: | IF A.3A/11 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - conference focus or acting as the notifier of event information.  |              |            |                |              |            |                |
| c23: | IF A.3A/52 THEN m ELSE (A.3/1 OR A.3/7A OR A.3/7B) AND A.4/23 THEN o ELSE n/a - - message waiting indication subscriber UA, UE, AS acting as terminating UA, or redirect server, AS acting as originating UA all as subscriber of event information. |              |            |                |              |            |                |
| c24: | IF A.3A/52 THEN m ELSE (A.3/1 OR A.3/7A OR A.3/7B) AND A.4/22 THEN o ELSE n/a - - message waiting indication notifier UA, UE, AS acting as terminating UA, or redirect server, AS acting as originating UA all as notifier of event information.     |              |            |                |              |            |                |
| c25: | IF A.4A/1 THEN (IF A.3/1 AND A.4/53 THEN m ELSE o) ELSE n/a - - reg event package, UE, reg event package extension for GRUUs.  |              |            |                |              |            |                |
| c26: | IF (A.3/7B OR A.3/1) AND (A.4/23 OR A.4/41) THEN o ELSE n/a - - AS acting as originating UA, UE, acting as the subscriber to event information, an event state publication extension to the session initiation protocol.                             |              |            |                |              |            |                |
| c27: | IF (A.4/22 OR A.4/41) AND A.3/1 THEN o ELSE n/a - - UE, acting as the notifier of event information, an event state publication extension to the session initiation protocol.  |              |            |                |              |            |                |
| c29: | IF A.4/104B THEN m ELSE n/a - - distribution of load filters.  |              |            |                |              |            |                |
| c30: | IF A.4/104B THEN IF A.3/4 OR A.3/7 OR A.3/9 THEN m ELSE n/a - - distribution of load filters. S-CSCF, IBCF, AS.  |              |            |                |              |            |                |
| c31: | IF A.4/104B THEN IF A.3/7 THEN m ELSE n/a - - distribution of load filters, AS.  |              |            |                |              |            |                |



Prerequisite A.4/13 - - SIP INFO method and package framework.

**Table A.4B: Supported info packages**

| Item | Does the implementation support  | Sender |            |                | Receiver |            |                |
|------|--|--------|------------|----------------|----------|------------|----------------|
|      |  | Ref.   | RFC status | Profile status | Ref.     | RFC status | Profile status |
| 1    | DTMF info package?   | 7.12.1 | n/a        | c1             | 7.12.1   | n/a        | c1             |
| 2    | g.3gpp.mid-call?   | [8M]   | n/a        | c2             | [8M]     | n/a        | c3             |
| 3    | g.3gpp.ussd?   | [8W]   | n/a        | c4             | [8W]     | n/a        | c4             |
| c1:  | IF A.3/6 OR A.3A/57 OR A.3A/58 OR A.3A/59 OR A.3A/60 THEN m ELSE o - - MGCF, customized alerting tones application server, customized alerting tones UA client, customized ringing signal application server, customized ringing signal UA client. |        |            |                |          |            |                |
| c2:  | IF A.3A/83 THEN o ELSE n/a - - SCC application server.   |        |            |                |          |            |                |
| c3:  | IF A.3A/81 THEN o ELSE n/a - - MSC server enhanced for ICS.  |        |            |                |          |            |                |
| c4:  | IF A.3A/92 OR A.3A/93 THEN m ELSE n/a - - USSI UE, USSI AS.  |        |            |                |          |            |                |

**Table A.4C: Supported media control packages**

| Item | Does the implementation support                                     | Sender |            |                | Receiver |            |                |
|------|---|--------|------------|----------------|----------|------------|----------------|
|      |   | Ref.   | RFC status | Profile status | Ref.     | RFC status | Profile status |
| 1    | msc-ivr/1.0   | [147]  |            | c1             | [147]    |            | c2             |
| 2    | msc-mixer/1.0   | [148]  |            | c1             | [148]    |            | c2             |
| 3    | mrp-publish/1.0   | [192]  |            | c3             | [192]    |            | c4             |
| c1:  | IF A.3/7D THEN o ELSE n/a - - AS performing 3rd party call control. |        |            |                |          |            |                |
| c2:  | IF A.3/8 THEN o ELSE n/a - - MRFC.                                  |        |            |                |          |            |                |
| c3:  | IF A.3/8 THEN o ELSE n/a - - MRFC.                                  |        |            |                |          |            |                |
| c4:  | IF A.3/8A THEN o ELSE n/a - - MRB.                                  |        |            |                |          |            |                |

## A.2.1.3 PDUs

Table A.5: Supported methods

| Item | PDU   | Sending        |            |                | Receiving      |            |                |
|------|---|----------------|------------|----------------|----------------|------------|----------------|
|      |   | Ref.           | RFC status | Profile status | Ref.           | RFC status | Profile status |
| 1    | ACK request   | [26] 13        | c10        | c10            | [26] 13        | c11        | c11            |
| 2    | BYE request   | [26] 15.1      | c12        | c12            | [26] 15.1      | c12        | c12            |
| 3    | BYE response  | [26] 15.1      | c12        | c12            | [26] 15.1      | c12        | c12            |
| 4    | CANCEL request  | [26] 9         | m          | m              | [26] 9         | m          | m              |
| 5    | CANCEL response   | [26] 9         | m          | m              | [26] 9         | m          | m              |
| 6    | INFO request  | [25] 4.2       | c21        | c21            | [25] 4.2       | c21        | c21            |
| 7    | INFO response   | [25] 4.2       | c21        | c21            | [25] 4.2       | c21        | c21            |
| 8    | INVITE request  | [26] 13        | c10        | c10            | [26] 13        | c11        | c11            |
| 9    | INVITE response   | [26] 13        | c11        | c11            | [26] 13        | c10        | c10            |
| 9A   | MESSAGE request   | [50] 4         | c7         | c7             | [50] 7         | c7         | c7             |
| 9B   | MESSAGE response  | [50] 4         | c7         | c7             | [50] 7         | c7         | c7             |
| 10   | NOTIFY request  | [28] 8.1.2     | c4         | c4             | [28] 8.1.2     | c3         | c3             |
| 11   | NOTIFY response   | [28] 8.1.2     | c3         | c3             | [28] 8.1.2     | c4         | c4             |
| 12   | OPTIONS request   | [26] 11        | m          | m              | [26] 11        | m          | m              |
| 13   | OPTIONS response  | [26] 11        | m          | m              | [26] 11        | m          | m              |
| 14   | PRACK request   | [27] 6         | c5         | c5             | [27] 6         | c5         | c5             |
| 15   | PRACK response  | [27] 6         | c5         | c5             | [27] 6         | c5         | c5             |
| 15A  | PUBLISH request   | [70]<br>11.1.3 | c20        | c20            | [70]<br>11.1.3 | c20        | c20            |
| 15B  | PUBLISH response  | [70]<br>11.1.3 | c20        | c20            | [70]<br>11.1.3 | c20        | c20            |
| 16   | REFER request   | [36] 3         | c1         | c1             | [36] 3         | c1         | c1             |
| 17   | REFER response  | [36] 3         | c1         | c1             | [36] 3         | c1         | c1             |
| 18   | REGISTER request  | [26] 10        | c8         | c8             | [26] 10        | c9         | c9             |
| 19   | REGISTER response   | [26] 10        | c9         | c9             | [26] 10        | c8         | c8             |
| 20   | SUBSCRIBE request   | [28] 8.1.1     | c3         | c3             | [28] 8.1.1     | c4         | c4             |
| 21   | SUBSCRIBE response  | [28] 8.1.1     | c4         | c4             | [28] 8.1.1     | c3         | c3             |
| 22   | UPDATE request  | [29] 6.1       | c6         | c6             | [29] 6.2       | c6         | c6             |
| 23   | UPDATE response   | [29] 6.2       | c6         | c6             | [29] 6.1       | c6         | c6             |
| c1:  | IF A.4/15 THEN m ELSE n/a -- the REFER method extension.  |                |            |                |                |            |                |
| c3:  | IF A.4/23 THEN m ELSE n/a -- recipient for event information.                                     |                |            |                |                |            |                |
| c4:  | IF A.4/22 THEN m ELSE n/a -- notifier of event information.                                       |                |            |                |                |            |                |
| c5:  | IF A.4/14 THEN m ELSE n/a -- reliability of provisional responses extension.                      |                |            |                |                |            |                |
| c6:  | IF A.4/17 THEN m ELSE n/a -- the SIP update method extension.                                     |                |            |                |                |            |                |
| c7:  | IF A.4/27 THEN m ELSE n/a -- the SIP MESSAGE method.  |                |            |                |                |            |                |
| c8:  | IF A.4/1 THEN m ELSE n/a -- client behaviour for registration.                                    |                |            |                |                |            |                |
| c9:  | IF A.4/2 THEN m ELSE n/a -- registrar.  |                |            |                |                |            |                |
| c10: | IF A.4/3 THEN m ELSE n/a -- client behaviour for INVITE requests.                                 |                |            |                |                |            |                |
| c11: | IF A.4/4 THEN m ELSE n/a -- server behaviour for INVITE requests.                                 |                |            |                |                |            |                |
| c12: | IF A.4/5 THEN m ELSE n/a -- session release.  |                |            |                |                |            |                |
| c20: | IF A.4/41 THEN m ELSE n/a -- event state publication extension.                                   |                |            |                |                |            |                |
| c21: | IF A.4/13 OR A.4/13A THEN m ELSE n/a -- SIP INFO method and package framework, legacy INFO usage. |                |            |                |                |            |                |

## A.2.1.4 PDU parameters

### A.2.1.4.1 Status-codes

**Table A.6: Supported status-codes**

| Item | Header                                 | Sending      |            |                | Receiving    |            |                |
|------|--|--------------|------------|----------------|--------------|------------|----------------|
|      |  | Ref.         | RFC status | Profile status | Ref.         | RFC status | Profile status |
| 1    | 100 (Trying)                           | [26] 21.1.1  | c21        | c21            | [26] 21.1.1  | c11        | c11            |
| 101  | 1xx response                           | [26] 21.1    | p21        | p21            | [26] 21.1    | p21        | p21            |
| 101A | 18x response                           | [26] 21.1    | p21        | p21            | [26] 21.1    | p21        | p21            |
| 2    | 180 (Ringing)                          | [26] 21.1.2  | c2         | c2             | [26] 21.1.2  | c1         | c1             |
| 3    | 181 (Call Is Being Forwarded)          | [26] 21.1.3  | c2         | c2             | [26] 21.1.3  | c1         | c1             |
| 4    | 182 (Queued)                           | [26] 21.1.4  | c2         | c2             | [26] 21.1.4  | c1         | c1             |
| 5    | 183 (Session Progress)                 | [26] 21.1.5  | c34        | c34            | [26] 21.1.5  | c1         | c1             |
| 5A   | 199 (Early Dialog Terminated)          | [142] 11.1   | c32        | c32            | [142] 11.1   | c32        | c32            |
| 102  | 2xx response                           | [26] 21.2    | p22        | p22            | [26] 21.1    | p22        | p22            |
| 6    | 200 (OK)                               | [26] 21.2.1  | m          | m              | [26] 21.2.1  | m          | m              |
| 7    | 202 (Accepted)                         | [28] 8.3.1   | c3         | c3             | [28] 8.3.1   | c3         | c3             |
| 103  | 3xx response                           | [26] 21.3    | p23        | p23            | [26] 21.1    | p23        | p23            |
| 8    | 300 (Multiple Choices)                 | [26] 21.3.1  | m          | m              | [26] 21.3.1  | m          | m              |
| 9    | 301 (Moved Permanently)                | [26] 21.3.2  | m          | m              | [26] 21.3.2  | m          | m              |
| 10   | 302 (Moved Temporarily)                | [26] 21.3.3  | m          | m              | [26] 21.3.3  | m          | m              |
| 11   | 305 (Use Proxy)                        | [26] 21.3.4  | m          | m              | [26] 21.3.4  | m          | m              |
| 12   | 380 (Alternative Service)              | [26] 21.3.5  | m          | m              | [26] 21.3.5  | m          | m              |
| 104  | 4xx response                           | [26] 21.4    | p24        | p24            | [26] 21.4    | p24        | p24            |
| 13   | 400 (Bad Request)                      | [26] 21.4.1  | m          | m              | [26] 21.4.1  | m          | m              |
| 14   | 401 (Unauthorized)                     | [26] 21.4.2  | o          | c12            | [26] 21.4.2  | m          | m              |
| 15   | 402 (Payment Required)                 | [26] 21.4.3  | n/a        | n/a            | [26] 21.4.3  | n/a        | n/a            |
| 16   | 403 (Forbidden)                        | [26] 21.4.4  | m          | m              | [26] 21.4.4  | m          | m              |
| 17   | 404 (Not Found)                        | [26] 21.4.5  | m          | m              | [26] 21.4.5  | m          | m              |
| 18   | 405 (Method Not Allowed)               | [26] 21.4.6  | m          | m              | [26] 21.4.6  | m          | m              |
| 19   | 406 (Not Acceptable)                   | [26] 21.4.7  | m          | m              | [26] 21.4.7  | m          | m              |
| 20   | 407 (Proxy Authentication Required)    | [26] 21.4.8  | o          | o              | [26] 21.4.8  | m          | m              |
| 21   | 408 (Request Timeout)                  | [26] 21.4.9  | c2         | c2             | [26] 21.4.9  | m          | m              |
| 22   | 410 (Gone)                             | [26] 21.4.10 | m          | m              | [26] 21.4.10 | m          | m              |
| 22A  | 412 (Conditional Request Failed)       | [70] 11.2.1  | c20        | c20            | [70] 11.2.1  | c20        | c20            |
| 23   | 413 (Request Entity Too Large)         | [26] 21.4.11 | m          | m              | [26] 21.4.11 | m          | m              |
| 24   | 414 (Request-URI Too Large)            | [26] 21.4.12 | m          | m              | [26] 21.4.12 | m          | m              |
| 25   | 415 (Unsupported Media Type)           | [26] 21.4.13 | m          | m              | [26] 21.4.13 | m          | m              |
| 26   | 416 (Unsupported URI Scheme)           | [26] 21.4.14 | m          | m              | [26] 21.4.14 | m          | m              |
| 26A  | 417 (Unknown Resource Priority)        | [116] 4.6.2  | c24        | c24            | [116] 4.6.2  | c24        | c24            |
| 27   | 420 (Bad Extension)                    | [26] 21.4.15 | m          | c13            | [26] 21.4.15 | m          | m              |
| 28   | 421 (Extension Required)               | [26] 21.4.16 | o          | o              | [26] 21.4.16 | i          | i              |
| 28A  | 422 (Session Interval Too Small)       | [58] 6       | c7         | c7             | [58] 6       | c7         | c7             |
| 29   | 423 (Interval Too Brief)               | [26] 21.4.17 | c4         | c4             | [26] 21.4.17 | m          | m              |
| 29A  | 424 (Bad Location Information)         | [89] 4.2     | c23        | c23            | [89] 4.2     | c23        | c23            |
| 29B  | 429 (Provide Referrer Identity)        | [59] 5       | c8         | c8             | [59] 5       | c9         | c9             |
| 29C  | 430 (Flow Failed)                      | [92] 11      | n/a        | n/a            | [92] 11      | c22        | c22            |
| 29D  | 433 (Anonymity Disallowed)             | [67] 4       | c14        | c14            | [67] 4       | c14        | c14            |
| 29E  | 439 (First Hop Lacks Outbound Support) | [92] 11      | c28        | c28            | [92] 11      | c29        | c29            |
| 29F  | 440 (Max Breadth Exceeded)             | [117] 5      | n/a        | c30            | [117] 5      | c31        | c31            |
| 29G  | 469 (Bad INFO Package)                 | [25] 4.2     | c33        | c33            | [25] 4.2     | c33        | c33            |
| 29H  | 470 (Consent Needed)                   | [125] 5.9.2  | c26        | c26            | [125] 5.9.2  | c27        | c27            |
| 30   | 480 (Temporarily Unavailable)          | [26] 21.4.18 | m          | m              | [26] 21.4.18 | m          | m              |

| Item | Header                                | Sending      |            |                | Receiving    |            |                |
|------|---------------------------------------|--------------|------------|----------------|--------------|------------|----------------|
|      |                                       | Ref.         | RFC status | Profile status | Ref.         | RFC status | Profile status |
| 31   | 481 (Call/Transaction Does Not Exist) | [26] 21.4.19 | m          | m              | [26] 21.4.19 | m          | m              |
| 32   | 482 (Loop Detected)                   | [26] 21.4.20 | m          | m              | [26] 21.4.20 | m          | m              |
| 33   | 483 (Too Many Hops)                   | [26] 21.4.21 | m          | m              | [26] 21.4.21 | m          | m              |
| 34   | 484 (Address Incomplete)              | [26] 21.4.22 | o          | o              | [26] 21.4.22 | m          | m              |
| 35   | 485 (Ambiguous)                       | [26] 21.4.23 | o          | o              | [26] 21.4.23 | m          | m              |
| 36   | 486 (Busy Here)                       | [26] 21.4.24 | m          | m              | [26] 21.4.24 | m          | m              |
| 37   | 487 (Request Terminated)              | [26] 21.4.25 | m          | m              | [26] 21.4.25 | m          | m              |
| 38   | 488 (Not Acceptable Here)             | [26] 21.4.26 | m          | m              | [26] 21.4.26 | m          | m              |
| 39   | 489 (Bad Event)                       | [28] 7.3.2   | c3         | c3             | [28] 7.3.2   | c3         | c3             |
| 40   | 491 (Request Pending)                 | [26] 21.4.27 | m          | m              | [26] 21.4.27 | m          | m              |
| 41   | 493 (Undecipherable)                  | [26] 21.4.28 | m          | m              | [26] 21.4.28 | m          | m              |
| 41A  | 494 (Security Agreement Required)     | [48] 2       | c5         | c5             | [48] 2       | c6         | c6             |
| 105  | 5xx response                          | [26] 21.5    | p25        | p25            | [26] 21.5    | p25        | p25            |
| 42   | 500 (Internal Server Error)           | [26] 21.5.1  | m          | m              | [26] 21.5.1  | m          | m              |
| 43   | 501 (Not Implemented)                 | [26] 21.5.2  | m          | m              | [26] 21.5.2  | m          | m              |
| 44   | 502 (Bad Gateway)                     | [26] 21.5.3  | o          | o              | [26] 21.5.3  | m          | m              |
| 45   | 503 (Service Unavailable)             | [26] 21.5.4  | m          | m              | [26] 21.5.4  | m          | m              |
| 46   | 504 (Server Time-out)                 | [26] 21.5.5  | m          | m              | [26] 21.5.5  | m          | m              |
| 47   | 505 (Version not supported)           | [26] 21.5.6  | m          | m              | [26] 21.5.6  | m          | m              |
| 48   | 513 (Message Too Large)               | [26] 21.5.7  | m          | m              | [26] 21.5.7  | m          | m              |
| 49   | 580 (Precondition Failure)            | [30] 8       | c35        | c35            | [30] 8       | c35        | c35            |
| 106  | 6xx response                          | [26] 21.6    | p26        | p26            | [26] 21.6    | p26        | p26            |
| 50   | 600 (Busy Everywhere)                 | [26] 21.6.1  | m          | m              | [26] 21.6.1  | m          | m              |
| 51   | 603 (Decline)                         | [26] 21.6.2  | c10        | c10            | [26] 21.6.2  | m          | m              |
| 52   | 604 (Does Not Exist Anywhere)         | [26] 21.6.3  | m          | m              | [26] 21.6.3  | m          | m              |
| 53   | 606 (Not Acceptable)                  | [26] 21.6.4  | m          | m              | [26] 21.6.4  | m          | m              |

| Item | Header   | Sending |            |                | Receiving |            |                |
|------|--|---------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| c1:  | IF A.5/9 THEN m ELSE n/a - - INVITE response.  |         |            |                |           |            |                |
| c2:  | IF A.5/9 THEN o ELSE n/a - - INVITE response.  |         |            |                |           |            |                |
| c3:  | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.   |         |            |                |           |            |                |
| c4:  | IF A.5/19 OR A.5/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response.   |         |            |                |           |            |                |
| c5:  | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.  |         |            |                |           |            |                |
| c6:  | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.  |         |            |                |           |            |                |
| c7:  | IF A.4/42 AND (A.5/9 OR A.5/23) THEN m ELSE n/a - - the SIP session timer AND (INVITE response OR UPDATE response).  |         |            |                |           |            |                |
| c8:  | IF A.4/43 AND A.5/17 THEN o ELSE n/a - - the SIP Referred-By mechanism and REFER response.   |         |            |                |           |            |                |
| c9:  | IF A.4/43 AND A.5/17 THEN m ELSE n/a - - the SIP Referred-By mechanism and REFER response.   |         |            |                |           |            |                |
| c10: | IF A.4/44 THEN m ELSE o - - the Session Initiation Protocol (SIP) "Replaces" header.   |         |            |                |           |            |                |
| c11: | IF A.5/3 OR A.5/9 OR A.5/9B OR A.5/11 OR A.5/13 OR A.5/15 OR A.5/15B OR A.5/17 OR A.5/19 OR A.5/21 OR A.5/23 THEN m ELSE n/a - - BYE response or INVITE response or MESSAGE response or NOTIFY response or OPTIONS response or PRACK response or PUBLISH response or REFER response or REGISTER response or SUBSCRIBE response or UPDATE response.   |         |            |                |           |            |                |
| c12: | IF A.3/4 THEN m ELSE o - - S-CSCF.   |         |            |                |           |            |                |
| c13: | IF A.3/1 OR A.3/2 OR A.3/4 THEN m ELSE o - - UE, P-CSCF, S-CSCF.   |         |            |                |           |            |                |
| c14: | IF A.4/48 THEN m ELSE n/a - - rejecting anonymous requests in the session initiation protocol.   |         |            |                |           |            |                |
| c20: | IF A.4/41 THEN m ELSE n/a - - an event state publication extension to the session initiation protocol.   |         |            |                |           |            |                |
| c21: | IF A.5/3 OR A.5/9 OR A.5/9B OR A.5/11 OR A.5/13 OR A.5/15 OR A.5/15B OR A.5/17 OR A.5/19 OR A.5/21 OR A.5/23 THEN o ELSE n/a - - BYE response or INVITE response or MESSAGE response or NOTIFY response or OPTIONS response or PRACK response or PUBLISH response or REFER response or REGISTER response or SUBSCRIBE response or UPDATE response.   |         |            |                |           |            |                |
| c22: | IF A.4/57 THEN m ELSE n/a - - managing client initiated connections in SIP.  |         |            |                |           |            |                |
| c23: | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.   |         |            |                |           |            |                |
| c24: | IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.  |         |            |                |           |            |                |
| c26: | IF A.4/75B THEN m ELSE n/a - - a recipient within the framework for consent-based communications in SIP.   |         |            |                |           |            |                |
| c27: | IF A.4/75A THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP.   |         |            |                |           |            |                |
| c28: | IF A.4/2 AND A.4/57 THEN m ELSE n/a - - registrar, managing client initiated connections in SIP.   |         |            |                |           |            |                |
| c29: | IF A.4/1 AND A.4/57 THEN m ELSE n/a - - client behaviour for registration, managing client initiated connections in SIP.   |         |            |                |           |            |                |
| c30: | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling).   |         |            |                |           |            |                |
| c31: | IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.  |         |            |                |           |            |                |
| c32: | IF A.5/9 AND A.4/81 THEN m ELSE n/a - - INVITE response and 199 (Early Dialog Terminated) response.  |         |            |                |           |            |                |
| c33: | IF A.4/13 THEN m ELSE n/a - - SIP INFO method and package framework.   |         |            |                |           |            |                |
| c34: | IF A.4/16 OR A.3/6 THEN m ELSE IF A.5/9 THEN o ELSE n/a - - initiating a session which require local and/or remote resource reservation, MGCF, INVITE response.  |         |            |                |           |            |                |
| c35: | IF A.4/16 THEN m ELSE n/a - - integration of resource management and SIP.  |         |            |                |           |            |                |
| p21: | A.6/2 OR A.6/3 OR A.6/4 OR A.6/5 OR A.6/5A - - 1xx response.   |         |            |                |           |            |                |
| p22: | A.6/6 OR A.6/7 - - 2xx response.   |         |            |                |           |            |                |
| p23: | A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 - - 3xx response.   |         |            |                |           |            |                |
| p24: | A.6/13 OR A.6/14 OR A.6/15 OR A.6/16 OR A.6/17 OR A.6/18 OR A.6/19 OR A.6/20 OR A.6/21 OR A.6/22 OR A.6/22A OR A.6/23 OR A.6/24 OR A.6/25 OR A.6/26 OR A.6/26A OR A.6/27 OR A.6/28 OR A.6/28A OR A.6/29 OR A.6/29A OR A.6/29B OR A.6/29C OR A.6/29D OR A.6/29E OR A.6/29F OR A.6/29G OR A.6/29H OR A.6/30 OR A.6/31 OR A.6/32 OR A.6/33 OR A.6/34 OR A.6/35 OR A.6/36 OR A.6/436 OR A.6/38 OR A.6/39 OR A.6/40 OR A.6/41 OR A.6/41A. - 4xx response. |         |            |                |           |            |                |
| p25: | A.6/42 OR A.6/43 OR A.6/44 OR A.6/45 OR A.6/46 OR A.6/47 OR A.6/48 OR A.6/49 - - 5xx response  |         |            |                |           |            |                |
| p26: | A.6/50 OR A.6/51 OR A.6/52 OR A.6/53 - - 6xx response.   |         |            |                |           |            |                |

#### A.2.1.4.2 ACK method

Prerequisite A.5/1 – ACK request

**Table A.7: Supported header fields within the ACK request**

| Item | Header field  | Sending                          |            |                | Receiving                        |            |                |
|------|---|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |   | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 1    | Accept-Contact  | [56B] 9.2                        | c9         | c9             | [56B] 9.2                        | c10        | c10            |
| 2    | Allow-Events  | [28] 7.2.2                       | c1         | c1             | [28] 7.2.2                       | c2         | c2             |
| 3    | Authorization   | [26] 20.7                        | c3         | c3             | [26] 20.7                        | c3         | c3             |
| 4    | Call-ID   | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 6    | Content-Disposition   | [26] 20.11                       | o          | o              | [26] 20.11                       | m          | m              |
| 7    | Content-Encoding  | [26] 20.12                       | o          | o              | [26] 20.12                       | m          | m              |
| 8    | Content-Language  | [26] 20.13                       | o          | o              | [26] 20.13                       | m          | m              |
| 9    | Content-Length  | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 10   | Content-Type  | [26] 20.15                       | m          | m              | [26] 20.15                       | m          | m              |
| 11   | CSeq  | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 12   | Date  | [26] 20.17                       | c4         | c4             | [26] 20.17                       | m          | m              |
| 13   | From  | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 13A  | Max-Breadth   | [117] 5.8                        | n/a        | c14            | [117] 5.8                        | c15        | c15            |
| 14   | Max-Forwards  | [26] 20.22                       | m          | m              | [26] 20.22                       | n/a        | c16            |
| 15   | MIME-Version  | [26] 20.24                       | o          | o              | [26] 20.24                       | m          | m              |
| 15A  | P-Access-Network-Info   | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c19        | c20            | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c19        | c21            |
| 15C  | Privacy   | [33] 4.2                         | c6         | n/a            | [33] 4.2                         | c6         | n/a            |
| 15D  | P-Charging-Vector   | [52] 4.6,<br>[52A] 4             | c22        | c23            | [52] 4.6,<br>[52A] 4             | c22        | c23            |
| 16   | Proxy-Authorization   | [26] 20.28                       | c5         | c5             | [26] 20.28                       | n/a        | n/a            |
| 17   | Proxy-Require   | [26] 20.29                       | o          | n/a            | [26] 20.29                       | n/a        | n/a            |
| 17A  | Reason  | [34A] 2                          | c8         | c8             | [34A] 2                          | c8         | c8             |
| 17B  | Recv-Info   | [25] 5.2.3                       | c17        | c17            | [25] 5.2.3                       | c17        | c17            |
| 17C  | Reject-Contact  | [56B] 9.2                        | c9         | c9             | [56B] 9.2                        | c10        | c10            |
| 17D  | Request-Disposition   | [56B] 9.1                        | c9         | c9             | [56B] 9.1                        | c10        | c10            |
| 18   | Require   | [26] 20.32                       | n/a        | n/a            | [26] 20.32                       | n/a        | n/a            |
| 18A  | Resource-Priority   | [116] 3.1                        | c11        | c11            | [116] 3.1                        | c11        | c11            |
| 19   | Route   | [26] 20.34                       | m          | m              | [26] 20.34                       | n/a        | c16            |
| 19A  | Session-ID  | [162]                            | o          | c18            | [162]                            | o          | c18            |
| 20   | Timestamp   | [26] 20.38                       | c7         | c7             | [26] 20.38                       | m          | m              |
| 21   | To  | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 22   | User-Agent  | [26] 20.41                       | o          | o              | [26] 20.41                       | m          | m              |
| 23   | Via   | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| c1:  | IF A.4/22 THEN o ELSE n/a -- acting as the notifier of event information.   |                                  |            |                |                                  |            |                |
| c2:  | IF A.4/23 THEN m ELSE n/a -- acting as the subscriber to event information.   |                                  |            |                |                                  |            |                |
| c3:  | IF A.4/7 THEN m ELSE n/a -- authentication between UA and UA.   |                                  |            |                |                                  |            |                |
| c4:  | IF A.4/11 THEN o ELSE n/a -- insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c5:  | IF A.4/8A THEN m ELSE n/a -- authentication between UA and proxy.   |                                  |            |                |                                  |            |                |
| c6:  | IF A.4/26 THEN o ELSE n/a -- a privacy mechanism for the Session Initiation Protocol (SIP).   |                                  |            |                |                                  |            |                |
| c7:  | IF A.4/6 THEN o ELSE n/a -- timestamping of requests.   |                                  |            |                |                                  |            |                |
| c8:  | IF A.4/38 THEN o ELSE n/a -- the Reason header field for the session initiation protocol.   |                                  |            |                |                                  |            |                |
| c9:  | IF A.4/40 THEN o ELSE n/a -- caller preferences for the session initiation protocol.  |                                  |            |                |                                  |            |                |
| c10: | IF A.4/40 THEN m ELSE n/a -- caller preferences for the session initiation protocol.  |                                  |            |                |                                  |            |                |
| c11: | IF A.4/70 THEN m ELSE n/a -- communications resource priority for the session initiation protocol.  |                                  |            |                |                                  |            |                |
| c14: | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE n/a -- addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling). |                                  |            |                |                                  |            |                |
| c15: | IF A.4/71 THEN m ELSE n/a -- addressing an amplification vulnerability in session initiation protocol forking proxies.  |                                  |            |                |                                  |            |                |
| c16: | IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o -- UE, UE performing the functions of an external attached network.   |                                  |            |                |                                  |            |                |
| c17: | IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a -- SIP INFO method and package framework, legacy INFO usage.   |                                  |            |                |                                  |            |                |
| c18: | IF A.4/91 THEN m ELSE n/a -- the Session-ID header.   |                                  |            |                |                                  |            |                |
| c19: | IF A.4/34 THEN o ELSE n/a -- the P-Access-Network-Info header extension.  |                                  |            |                |                                  |            |                |
| c20: | IF A.4/34 AND A.3/1 OR A.3/2A OR A.3/7 OR A.3A/81 THEN m ELSE n/a -- the P-Access-Network-Info header extension and UE, P-CSCF (IMS-ALG), AS, MSC Server enhanced for ICS.  |                                  |            |                |                                  |            |                |
| c21: | IF A.4/34 AND A.3/1 OR A.3/7 THEN m ELSE n/a -- the P-Access-Network-Info header extension and UE, AS.  |                                  |            |                |                                  |            |                |
| c22: | IF A.4/36 THEN o ELSE n/a -- the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c23: | IF A.4/36 THEN o ELSE n/a -- the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |



Prerequisite A.5/1 – ACK request

**Table A.8: Supported message bodies within the ACK request**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

### A.2.1.4.3 BYE method

Prerequisite A.5/2 - - BYE request

**Table A.9: Supported header fields within the BYE request**

| Item | Header field                  | Sending           |            |                | Receiving         |            |                |
|------|-------------------------------|-------------------|------------|----------------|-------------------|------------|----------------|
|      |                               | Ref.              | RFC status | Profile status | Ref.              | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1         | o          | o              | [26] 20.1         | m          | m              |
| 1A   | Accept-Contact                | [56B] 9.2         | c18        | c18            | [56B] 9.2         | c22        | c22            |
| 2    | Accept-Encoding               | [26] 20.2         | o          | o              | [26] 20.2         | m          | m              |
| 3    | Accept-Language               | [26] 20.3         | o          | o              | [26] 20.3         | m          | m              |
| 3A   | Allow                         | [26] 20.5         | o          | o              | [26] 20.5         | m          | m              |
| 4    | Allow-Events                  | [28] 7.2.2        | c1         | c1             | [28] 7.2.2        | c2         | c2             |
| 5    | Authorization                 | [26] 20.7         | c3         | c3             | [26] 20.7         | c3         | c3             |
| 6    | Call-ID                       | [26] 20.8         | m          | m              | [26] 20.8         | m          | m              |
| 7    | Content-Disposition           | [26] 20.11        | o          | o              | [26] 20.11        | m          | m              |
| 8    | Content-Encoding              | [26] 20.12        | o          | o              | [26] 20.12        | m          | m              |
| 9    | Content-Language              | [26] 20.13        | o          | o              | [26] 20.13        | m          | m              |
| 10   | Content-Length                | [26] 20.14        | m          | m              | [26] 20.14        | m          | m              |
| 11   | Content-Type                  | [26] 20.15        | m          | m              | [26] 20.15        | m          | m              |
| 12   | CSeq                          | [26] 20.16        | m          | m              | [26] 20.16        | m          | m              |
| 13   | Date                          | [26] 20.17        | c4         | c4             | [26] 20.17        | m          | m              |
| 14   | From                          | [26] 20.20        | m          | m              | [26] 20.20        | m          | m              |
| 14A  | Geolocation                   | [89] 4.1          | c23        | c23            | [89] 4.1          | c23        | c23            |
| 14B  | Geolocation-Routing           | [89] 4.2          | c23        | c23            | [89] 4.2          | c23        | c23            |
| 14C  | Max-Breadth                   | [117] 5.8         | n/a        | c29            | [117] 5.8         | c30        | c30            |
| 15   | Max-Forwards                  | [26] 20.22        | m          | m              | [26] 20.22        | n/a        | c31            |
| 16   | MIME-Version                  | [26] 20.24        | o          | o              | [26] 20.24        | m          | m              |
| 16A  | P-Access-Network-Info         | [52] 4.4, [234] 2 | c9         | c10            | [52] 4.4, [234] 2 | c9         | c11            |
| 16B  | P-Asserted-Identity           | [34] 9.1          | n/a        | n/a            | [34] 9.1          | c6         | c6             |
| 16C  | P-Charging-Function-Addresses | [52] 4.5          | c13        | c14            | [52] 4.5          | c13        | c14            |
| 16D  | P-Charging-Vector             | [52] 4.6          | c12        | n/a            | [52] 4.6          | c12        | n/a            |
| 16F  | P-Preferred-Identity          | [34] 9.2          | c6         | x              | [34] 9.2          | n/a        | n/a            |
| 16G  | Privacy                       | [33] 4.2          | c7         | n/a            | [33] 4.2          | c7         | c7             |
| 17   | Proxy-Authorization           | [26] 20.28        | c5         | c5             | [26] 20.28        | n/a        | n/a            |
| 18   | Proxy-Require                 | [26] 20.29        | o          | n/a            | [26] 20.29        | n/a        | n/a            |
| 18A  | Reason                        | [34A] 2           | c17        | c21            | [34A] 2           | c24        | c24            |
| 19   | Record-Route                  | [26] 20.30        | n/a        | c31            | [26] 20.30        | n/a        | c31            |
| 19A  | Referred-By                   | [59] 3            | c19        | c19            | [59] 3            | c20        | c20            |
| 19B  | Reject-Contact                | [56B] 9.2         | c18        | c18            | [56B] 9.2         | c22        | c22            |
| 19C  | Request-Disposition           | [56B] 9.1         | c18        | c18            | [56B] 9.1         | c22        | c22            |
| 20   | Require                       | [26] 20.32        | m          | m              | [26] 20.32        | m          | m              |
| 20A  | Resource-Priority             | [116] 3.1         | c25        | c25            | [116] 3.1         | c25        | c25            |
| 21   | Route                         | [26] 20.34        | m          | m              | [26] 20.34        | n/a        | c31            |
| 21A  | Security-Client               | [48] 2.3.1        | c15        | c15            | [48] 2.3.1        | n/a        | n/a            |
| 21B  | Security-Verify               | [48] 2.3.1        | c16        | c16            | [48] 2.3.1        | n/a        | n/a            |
| 21C  | Session-ID                    | [162]             | o          | c32            | [162]             | o          | c32            |
| 22   | Supported                     | [26] 20.37        | o          | o              | [26] 20.37        | m          | m              |
| 23   | Timestamp                     | [26] 20.38        | c8         | c8             | [26] 20.38        | m          | m              |
| 24   | To                            | [26] 20.39        | m          | m              | [26] 20.39        | m          | m              |
| 25   | User-Agent                    | [26] 20.41        | o          | o              | [26] 20.41        | o          | o              |
| 25A  | User-to-User                  | [126] 7           | c26        | c26            | [126] 7           | c26        | c26            |
| 26   | Via                           | [26] 20.42        | m          | m              | [20] 20.42        | m          | m              |

|       |   |
|-------|---|
| c1:   | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.  |
| c2:   | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.  |
| c3:   | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.  |
| c4:   | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.  |
| c5:   | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.  |
| c6:   | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c7:   | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c8:   | IF A.4/6 THEN o ELSE n/a - - timestamping of requests.  |
| c9:   | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.   |
| c10:  | IF A.4/34 AND (A.3/1 OR A.3/2A OR A.3/7) THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE, P-CSCF (IMS-ALG) or AS.   |
| c11:  | IF A.4/34 AND (A.3/2A OR A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF (IMS-ALG), AS acting as terminating UA, AS acting as third-party call controller or EATF.  |
| c12:  | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.   |
| c13:  | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c14:  | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c15:  | IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note).   |
| c16:  | IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |
| c17:  | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c18:  | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.   |
| c19:  | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c20:  | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.  |
| c21:  | IF A.3/2 THEN m ELSE IF A.4/38 THEN o ELSE n/a - - P-CSCF, the Reason header field for the session initiation protocol.   |
| c22:  | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c23:  | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.  |
| c24:  | IF A.4/38 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c25:  | IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.  |
| c26:  | IF A.4/76 THEN o ELSE n/a - - transporting user to user information for call centers using SIP.   |
| c29:  | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network. |
| c30:  | IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |
| c31:  | IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.  |
| c32:  | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.  |
| NOTE: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].   |

Prerequisite A.5/2 - - BYE request

**Table A.10: Supported message bodies within the BYE request**

| Item | Header  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | XML Schema for PSTN   | [11B]     |            | c1             | [11B]     |            | c1             |
| 2    | VoiceXML expr / namelist data   | [145] 4.2 | m          | c2             | [145] 4.2 | m          | c2             |
| 3    | application/vnd.3gpp.ussd   | [8W]      |            | c3             | [8W]      |            | c4             |
| c1:  | IF A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9B OR A.3/13B THEN o ELSE n/a - - MGCF, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, IBCF (IMS-ALG), ISC gateway function (IMS-ALG). |           |            |                |           |            |                |
| c2:  | IF A.4/84 THEN m ELSE n/a - - SIP Interface to VoiceXML Media Services.   |           |            |                |           |            |                |
| c3:  | IF A.3A/93 OR A.3/9 OR A.3/2 OR A.3A/89 THEN m ELSE n/a - - USSI AS, IBCF, P-CSCF, ATCF (UA).   |           |            |                |           |            |                |
| c4:  | IF A.3A/92 OR A.3/9 OR A.3/2 OR A.3A/89 THEN m ELSE n/a - - USSI UE, IBCF, P-CSCF, ATCF (UA).   |           |            |                |           |            |                |

**Table A.11: Void**

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/1 - - Additional for 100 (Trying) response

**Table A.11A: Supported header fields within the BYE response**

| Item   | Header field   | Sending    |            |                | Receiving  |            |                |
|--|----------------|------------|------------|----------------|------------|------------|----------------|
|  |                | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1  | Call-ID        | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2  | Content-Length | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3  | CSeq           | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4  | Date           | [26] 20.17 | c1         | c1             | [26] 20.17 | m          | m              |
| 5  | From           | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6  | To             | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7  | Via            | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |                |            |            |                |            |            |                |

Prerequisite A.5/3 - - BYE response for all remaining status-codes

**Table A.12: Supported header fields within the BYE response**

| Item  | Header field   | Sending                          |            |                | Receiving                        |            |                |
|-------|--|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|       |  | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A    | Allow  | [26] 20.5                        | c11        | c11            | [26] 20.5                        | m          | m              |
| 1     | Call-ID  | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 2     | Content-Disposition  | [26] 20.11                       | o          | o              | [26] 20.11                       | m          | m              |
| 3     | Content-Encoding   | [26] 20.12                       | o          | o              | [26] 20.12                       | m          | m              |
| 4     | Content-Language   | [26] 20.13                       | o          | o              | [26] 20.13                       | m          | m              |
| 5     | Content-Length   | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6     | Content-Type   | [26] 20.15                       | m          | m              | [26] 20.15                       | m          | m              |
| 7     | CSeq   | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8     | Date   | [26] 20.17                       | c1         | c1             | [26] 20.17                       | m          | m              |
| 9     | From   | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A    | Geolocation-Error  | [89] 4.3                         | c12        | c12            | [89] 4.3                         | c12        | c12            |
| 10    | MIME-Version   | [26] 20.24                       | o          | o              | [26] 20.24                       | m          | m              |
| 10A   | P-Access-Network-Info  | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c6             | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c7             |
| 10B   | P-Asserted-Identity  | [34] 9.1                         | n/a        | n/a            | [34] 9.1                         | c3         | c3             |
| 10C   | P-Charging-Function-Addresses  | [52] 4.5,<br>[52A] 4             | c9         | c10            | [52] 4.5,<br>[52A] 4             | c9         | c10            |
| 10D   | P-Charging-Vector  | [52] 4.6,<br>[52A] 4             | c8         | n/a            | [52] 4.6,<br>[52A] 4             | c8         | n/a            |
| 10E   | P-Preferred-Identity   | [34] 9.2                         | c3         | x              | [34] 9.2                         | n/a        | n/a            |
| 10F   | Privacy  | [33] 4.2                         | c4         | n/a            | [33] 4.2                         | c4         | c4             |
| 10G   | Require  | [26] 20.32                       | m          | m              | [26] 20.32                       | m          | m              |
| 10H   | Server   | [26] 20.35                       | o          | o              | [26] 20.35                       | o          | o              |
| 10I   | Session-ID   | [162]                            | o          | c16            | [162]                            | o          | c16            |
| 11    | Timestamp  | [26] 20.38                       | m          | m              | [26] 20.38                       | c2         | c2             |
| 12    | To   | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 12A   | User-Agent   | [26] 20.41                       | o          | o              | [26] 20.41                       | o          | o              |
| 12B   | User-to-User   | [126] 7                          | c13        | c13            | [126] 7                          | c13        | c13            |
| 13    | Via  | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 14    | Warning  | [26] 20.43                       | o (note)   | o (note)       | [26] 20.43                       | o          | o              |
| c1:   | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c2:   | IF A.4/6 THEN m ELSE n/a - - timestamping of requests.   |                                  |            |                |                                  |            |                |
| c3:   | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.   |                                  |            |                |                                  |            |                |
| c4:   | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |                                  |            |                |                                  |            |                |
| c5:   | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.  |                                  |            |                |                                  |            |                |
| c6:   | IF A.4/34 AND (A.3/1 OR A.3/2A OR A.3/7) THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE, P-CSCF (IMS-ALG), or AS.   |                                  |            |                |                                  |            |                |
| c7:   | IF A.4/34 AND (A.3/2A OR A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF (IMS-ALG), AS acting as terminating UA, AS acting as third-party call controller or EATF. |                                  |            |                |                                  |            |                |
| c8:   | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c9:   | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c10:  | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c11:  | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).  |                                  |            |                |                                  |            |                |
| c12:  | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.   |                                  |            |                |                                  |            |                |
| c13:  | IF A.4/76 THEN o ELSE n/a - - transporting user to user information for call centers using SIP.  |                                  |            |                |                                  |            |                |
| c16:  | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |
| NOTE: | For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.  |                                  |            |                |                                  |            |                |

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.13: Supported header fields within the BYE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Accept-Resource-Priority   | [116] 3.2  | c5         | c5             | [116] 3.2  | c5         | c5             |
| 0B   | Allow-Events   | [28] 7.2.2 | c3         | c3             | [28] 7.2.2 | c4         | c4             |
| 1    | Authentication-Info  | [26] 20.6  | c1         | c1             | [26] 20.6  | c2         | c2             |
|      |  |            |            |                |            |            |                |
| 4    | Supported  | [26] 20.37 | o          | m              | [26] 20.37 | m          | m              |
| c1:  | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c2:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c3:  | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.   |            |            |                |            |            |                |
| c4:  | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.   |            |            |                |            |            |                |
| c5:  | IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol. |            |            |                |            |            |                |

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.13A: Supported header fields within the BYE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | o          | o              | [26] 20.18 | o          | o              |

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.14: Supported header fields within the BYE response**

| Item  | Header field  | Sending    |            |                | Receiving  |            |                |
|-------|---|------------|------------|----------------|------------|------------|----------------|
|       |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0B    | Contact   | [26] 20.10 | o (note)   | o              | [26] 20.10 | m          | m              |
| NOTE: | RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL. |            |            |                |            |            |                |

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.15: Supported header fields within the BYE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate  | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 8    | WWW-Authenticate  | [26] 20.44 | m          | m              | [26] 20.44 | m          | m              |
| c1:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.16: Supported header fields within the BYE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | o              |

**Table A.17: Void**

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/19 - - Additional for 407 (Proxy Authentication Required) response

**Table A.18: Supported header fields within the BYE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate  | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 6    | WWW-Authenticate  | [26] 20.44 | o          | o              | [26] 20.44 | o          | o              |
| c1:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/3 - - BYE response

Prerequisite A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.19: Supported header fields within the BYE response**

| Item | Header field                                     | Sending   |            |                | Receiving |            |                |
|------|--|-----------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept   | [26] 20.1 | o.1        | o.1            | [26] 20.1 | m          | m              |
| 2    | Accept-Encoding                                  | [26] 20.2 | o.1        | o.1            | [26] 20.2 | m          | m              |
| 3    | Accept-Language                                  | [26] 20.3 | o.1        | o.1            | [26] 20.3 | m          | m              |
| o.1  | At least one of these capabilities is supported. |           |            |                |           |            |                |



Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.19A: Supported header fields within the BYE response**

| Item | Header field   | Sending   |            |                | Receiving |            |                |
|------|--|-----------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority   | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.20: Supported header fields within the BYE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | m          | m              |

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.20A: Supported header fields within the BYE response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | x          | x              | [48] 2    | c1         | c1             |
| c1:  | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

**Table A.21: Void**

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/6 - - Additional for 200 (OK) response

**Table A.22: Supported message bodies within the BYE response**

| Item | Header  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | VoiceXML expr / namelist data   | [145] 4.2 | o          | c1             | [145] 4.2 | o          | c1             |
| c1:  | IF A.4/84 THEN o ELSE n/a - - SIP Interface to VoiceXML Media Services. |           |            |                |           |            |                |

## A.2.1.4.4 CANCEL method

Prerequisite A.5/4 - - CANCEL request

Table A.23: Supported header fields within the CANCEL request

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Accept-Contact   | [56B] 9.2  | c9         | c9             | [56B] 9.2  | c11        | c11            |
| 5    | Authorization  | [26] 20.7  | c3         | c3             | [26] 20.7  | c3         | c3             |
| 6    | Call-ID  | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 8    | Content-Length   | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 9    | CSeq   | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 10   | Date   | [26] 20.17 | c4         | c4             | [26] 20.17 | m          | m              |
| 11   | From   | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 11A  | Max-Breadth  | [117] 5.8  | n/a        | c16            | [117] 5.8  | c17        | c17            |
| 12   | Max-Forwards   | [26] 20.22 | m          | m              | [26] 20.22 | n/a        | c18            |
| 14   | Privacy  | [33] 4.2   | c6         | n/a            | [33] 4.2   | c6         | n/a            |
| 15   | Reason   | [34A] 2    | c7         | c10            | [34A] 2    | c12        | c12            |
| 16   | Record-Route   | [26] 20.30 | n/a        | c18            | [26] 20.30 | n/a        | c18            |
| 17   | Reject-Contact   | [56B] 9.2  | c9         | c9             | [56B] 9.2  | c11        | c11            |
| 17A  | Request-Disposition  | [56B] 9.1  | c9         | c9             | [56B] 9.1  | c11        | c11            |
| 17B  | Resource-Priority  | [116] 3.1  | c13        | c13            | [116] 3.1  | c13        | c13            |
| 18   | Route  | [26] 20.34 | m          | m              | [26] 20.34 | n/a        | c18            |
| 18A  | Session-ID   | [162]      | o          | c19            | [162]      | o          | c19            |
| 19   | Supported  | [26] 20.37 | o          | o              | [26] 20.37 | m          | m              |
| 20   | Timestamp  | [26] 20.38 | c8         | c8             | [26] 20.38 | m          | m              |
| 21   | To   | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 22   | User-Agent   | [26] 20.41 | o          | o              | [26] 20.41 | o          | o              |
| 23   | Via  | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c3:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c4:  | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.   |            |            |                |            |            |                |
| c6:  | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |            |            |                |            |            |                |
| c7:  | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.   |            |            |                |            |            |                |
| c8:  | IF A.4/6 THEN o ELSE n/a - - timestamping of requests.   |            |            |                |            |            |                |
| c9:  | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.  |            |            |                |            |            |                |
| c10: | IF A.3/2 THEN m ELSE IF A.4/38 THEN o ELSE n/a - - P-CSCF, the Reason header field for the session initiation protocol.  |            |            |                |            |            |                |
| c11: | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.  |            |            |                |            |            |                |
| c12: | IF A.4/38 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.   |            |            |                |            |            |                |
| c13: | IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.   |            |            |                |            |            |                |
| c16: | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network.. |            |            |                |            |            |                |
| c17: | IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.  |            |            |                |            |            |                |
| c18: | IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.   |            |            |                |            |            |                |
| c19: | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.   |            |            |                |            |            |                |

Prerequisite A.5/4 - - CANCEL request

Table A.24: Supported message bodies within the CANCEL request

| Item | Header  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | XML Schema for PSTN   | [11B]   |            | c1             | [11B]     |            | c1             |
| c1:  | IF A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9B OR A.3/13B THEN o ELSE n/a - - MGCF, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, IBCF (IMS-ALG), ISC gateway function (IMS-ALG). |         |            |                |           |            |                |

Prerequisite A.5/5 - - CANCEL response for all status-codes

**Table A.25: Supported header fields within the CANCEL response**

| Item  | Header field  | Sending    |            |                | Receiving  |            |                |
|-------|---|------------|------------|----------------|------------|------------|----------------|
|       |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1     | Call-ID   | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2     | Content-Length  | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3     | CSeq  | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4     | Date  | [26] 20.17 | c1         | c1             | [26] 20.17 | m          | m              |
| 5     | From  | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 5B    | Privacy   | [33] 4.2   | c3         | n/a            | [33] 4.2   | c3         | n/a            |
| 5C    | Session-ID  | [162]      | o          | c6             | [162]      | o          | c6             |
| 6     | Timestamp   | [26] 20.38 | m          | m              | [26] 20.38 | c2         | c2             |
| 7     | To  | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7A    | User-Agent  | [26] 20.41 | o          | o              | [26] 20.41 | o          | o              |
| 8     | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| 9     | Warning   | [26] 20.43 | o (note)   | o              | [26] 20.43 | o          | o              |
| c1:   | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.  |            |            |                |            |            |                |
| c2:   | IF A.4/6 THEN m ELSE n/a - - timestamping of requests.  |            |            |                |            |            |                |
| c3:   | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).                            |            |            |                |            |            |                |
| c6:   | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.  |            |            |                |            |            |                |
| NOTE: | For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL. |            |            |                |            |            |                |

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.26: Supported header fields within the CANCEL response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Accept-Resource-Priority   | [116] 3.2  | c1         | c1             | [116] 3.2  | c1         | c1             |
| 2    | Record-Route   | [26] 20.30 | n/a        | n/a            | [26] 20.30 | n/a        | n/a            |
| 4    | Supported  | [26] 20.37 | o          | m              | [26] 20.37 | m          | m              |
| c1:  | IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol. |            |            |                |            |            |                |

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.26A: Supported header fields within the CANCEL response**

| Item | Header     | Sending    |            |                | Receiving  |            |                |
|------|------------|------------|------------|----------------|------------|------------|----------------|
|      |            | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info | [26] 20.18 | o          | o              | [26] 20.18 | o          | o              |

**Table A.27: Void**

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.28: Supported header fields within the CANCEL response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | o              |

**Table A.29: Void**

**Table A.30: Void**

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.30A: Supported header fields within the CANCEL response**

| Item | Header field             | Sending  |            |                | Receiving |            |                |
|------|--------------------------|--|------------|----------------|-----------|------------|----------------|
|      |                          | Ref.   | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority | [116] 3.2  | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  |                          | IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol. |            |                |           |            |                |

Prerequisite A.5/5 - - CANCEL response

**Table A.31: Supported message bodies within the CANCEL response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

## A.2.1.4.5 COMET method

Void

## A.2.1.4.6 INFO method

Prerequisite A.5/9A - - INFO request

**Table A.32: Supported header fields within the INFO request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | o          | o              | [26] 20.1            | m          | m              |
| 2    | Accept-Encoding               | [26] 20.2            | o          | o              | [26] 20.2            | m          | m              |
| 3    | Accept-Language               | [26] 20.3            | o          | o              | [26] 20.3            | m          | m              |
| 4    | Allow                         | [26] 20.5            | o          | o              | [26] 20.5            | m          | m              |
| 5    | Allow-Events                  | [28] 7.2.2           | c1         | c1             | [28] 7.2.2           | c2         | c2             |
| 6    | Authorization                 | [26] 20.7            | c3         | c3             | [26] 20.7            | c3         | c3             |
| 7    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 7A   | Call-Info                     | [26] 20.9            | o          | o              | [26] 20.9            | o          | o              |
| 9    | Content-Disposition           | [26] 20.11           | o          | o              | [26] 20.11           | m          | m              |
| 10   | Content-Encoding              | [26] 20.12           | o          | o              | [26] 20.12           | m          | m              |
| 11   | Content-Language              | [26] 20.13           | o          | o              | [26] 20.13           | m          | m              |
| 12   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 13   | Content-Type                  | [26] 20.15           | m          | m              | [26] 29.15           | m          | m              |
| 14   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 15   | Date                          | [26] 20.17           | c4         | c4             | [26] 20.17           | m          | m              |
| 16   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 17   | Geolocation                   | [89] 4.1             | c29        | c29            | [89] 4.1             | c29        | c29            |
| 17A  | Geolocation-Routing           | [89] 4.2             | c29        | c29            | [89] 4.2             | c29        | c29            |
| 18   | Info-Package                  | [25] 7.2             | c42        | c42            | [25] 7.2             | c42        | c42            |
| 19   | Max-Breadth                   | [117] 5.8            | n/a        | c39            | [117] 5.8            | c40        | c40            |
| 20   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | n/a        | c41            |
| 21   | MIME-Version                  | [26] 20.24           | o          | o              | [26] 20.24           | m          | m              |
| 22   | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c15        | c16            | [52] 4.4,<br>[234] 2 | c15        | c17            |
| 23   | P-Charging-Function-Addresses | [52] 4.5             | c20        | c21            | [52] 4.5             | c20        | c21            |
| 24   | P-Charging-Vector             | [52] 4.6             | c18        | c19            | [52] 4.6             | c18        | c19            |
| 26   | Privacy                       | [33] 4.2             | c12        | c12            | [33] 4.2             | c12        | c12            |
| 27   | Proxy-Authorization           | [26] 20.28           | c5         | c5             | [26] 20.28           | n/a        | n/a            |
| 28   | Proxy-Require                 | [26] 20.29           | o          | n/a            | [26] 20.29           | n/a        | n/a            |
| 29   | Reason                        | [34A] 2              | c6         | c6             | [34A] 2              | c6         | c6             |
| 30   | Record-Route                  | [26] 20.30           | n/a        | c41            | [26] 20.30           | n/a        | c41            |
| 31   | Referred-By                   | [59] 3               | c25        | c25            | [59] 3               | c26        | c26            |
| 33   | Request-Disposition           | [56B] 9.1            | c24        | c24            | [56B] 9.1            | c28        | c28            |
| 34   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | m          | m              |
| 35   | Resource-Priority             | [116] 3.1            | c30        | c30            | [116] 3.1            | c30        | c30            |
| 36   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | n/a        | c41            |
| 37   | Security-Client               | [48] 2.3.1           | c22        | c22            | [48] 2.3.1           | n/a        | n/a            |
| 38   | Security-Verify               | [48] 2.3.1           | c23        | c23            | [48] 2.3.1           | n/a        | n/a            |
| 38A  | Session-ID                    | [162]                | o          | c43            | [162]                | o          | c43            |
| 39   | Subject                       | [26] 20.35           | o          | o              | [26] 20.36           | o          | o              |
| 40   | Supported                     | [26] 20.37           | m          | m              | [26] 20.37           | m          | m              |
| 41   | Timestamp                     | [26] 20.38           | c10        | c10            | [26] 20.38           | m          | m              |
| 42   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 43   | User-Agent                    | [26] 20.41           | o          | o              | [26] 20.41           | o          | o              |
| 44   | Via                           | [26] 20.42           | m          | m              | [26] 20.42           | m          | m              |

| Item    | Header field  | Sending |            |                | Receiving |            |                |
|---------|---|---------|------------|----------------|-----------|------------|----------------|
|         |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| c1:     | IF A.4/22 THEN o ELSE n/a   |         |            |                |           |            |                |
| c2:     | IF A.4/23 THEN m ELSE n/a   |         |            |                |           |            |                |
| c3:     | IF A.4/7 THEN m ELSE n/a  |         |            |                |           |            |                |
| c4:     | IF A.4/11 THEN o ELSE n/a   |         |            |                |           |            |                |
| c5:     | IF A.4/8A THEN m ELSE n/a   |         |            |                |           |            |                |
| c6:     | IF A.4/38 THEN o ELSE n/a   |         |            |                |           |            |                |
| c10:    | IF A.4/6 THEN o ELSE n/a  |         |            |                |           |            |                |
| c12:    | IF A.4/26 THEN o ELSE n/a   |         |            |                |           |            |                |
| c15:    | IF A.4/34 THEN o ELSE n/a   |         |            |                |           |            |                |
| c16:    | IF A.4/34 AND A.3/1 THEN m ELSE n/a   |         |            |                |           |            |                |
| c17:    | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a  |         |            |                |           |            |                |
| c18:    | IF A.4/36 THEN o ELSE n/a   |         |            |                |           |            |                |
| c19:    | IF A.4/36 THEN m ELSE n/a   |         |            |                |           |            |                |
| c20:    | IF A.4/35 THEN o ELSE n/a   |         |            |                |           |            |                |
| c21:    | IF A.4/35 THEN m ELSE n/a   |         |            |                |           |            |                |
| c22:    | IF A.4/37 OR A.4/37A THEN o ELSE n/a  |         |            |                |           |            |                |
| c23:    | IF A.4/37 OR A.4/37A THEN m ELSE n/a  |         |            |                |           |            |                |
| c24:    | IF A.4/40 THEN o ELSE n/a   |         |            |                |           |            |                |
| c25:    | IF A.4/43 THEN m ELSE n/a   |         |            |                |           |            |                |
| c26:    | IF A.4/43 THEN o ELSE n/a   |         |            |                |           |            |                |
| c28:    | IF A.4/40 THEN m ELSE n/a   |         |            |                |           |            |                |
| c29:    | IF A.4/60 THEN m ELSE n/a   |         |            |                |           |            |                |
| c30:    | IF A.4/70A THEN m ELSE n/a  |         |            |                |           |            |                |
| c39:    | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o  |         |            |                |           |            |                |
| c40:    | IF A.4/71 THEN m ELSE n/a   |         |            |                |           |            |                |
| c41:    | IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o   |         |            |                |           |            |                |
| c42:    | IF A.4/13A THEN n/a ELSE m  |         |            |                |           |            |                |
| c43:    | IF A.4/91 THEN m ELSE n/a   |         |            |                |           |            |                |
| NOTE 2: | Support of this header field in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header field in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19]. |         |            |                |           |            |                |

Prerequisite A.5/9A - - INFO request

**Table A.33: Supported message bodies within the INFO request**

| Item | Header       | Sending |            |                | Receiving |            |                |
|------|--------------|---------|------------|----------------|-----------|------------|----------------|
|      |              | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Info-Package | [25]    | m          | m              | [25]      | m          | m              |

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/1 - - Additional for 100 (Trying) response

**Table A.34: Supported header fields within the INFO response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID  | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length   | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq   | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date   | [26] 20.17 | c1         | c1             | [26] 20.17 | m          | m              |
| 5    | From   | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
|      |  |            |            |                |            |            |                |
| 6    | To   | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via  | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |            |            |                |            |            |                |



Prerequisite A.5/9B - - INFO response for all remaining status-codes

**Table A.35: Supported header fields within the INFO response**

| Item | Header field   | Sending                          |            |                | Receiving                        |            |                |
|------|--|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |  | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow  | [26] 20.5                        | c12        | c12            | [26] 20.5                        | m          | m              |
| 1    | Call-ID  | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 2    | Call-Info  | [26] 20.9                        | o          | o              | [26] 20.9                        | o          | o              |
| 3    | Content-Disposition  | [26] 20.11                       | o          | o              | [26] 20.11                       | m          | m              |
| 4    | Content-Encoding   | [26] 20.12                       | o          | o              | [26] 20.12                       | m          | m              |
| 5    | Content-Language   | [26] 20.13                       | o          | o              | [26] 20.13                       | m          | m              |
| 6    | Content-Length   | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 7    | Content-Type   | [26] 20.15                       | m          | m              | [26] 20.15                       | m          | m              |
| 8    | CSeq   | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 9    | Date   | [26] 20.17                       | c1         | c1             | [26] 20.17                       | m          | m              |
| 10   | From   | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 11   | Geolocation-Error  | [89] 4.3                         | c14        | c14            | [89] 4.3                         | c14        | c14            |
| 12   | MIME-Version   | [26] 20.24                       | o          | o              | [26] 20.24                       | m          | m              |
| 13   | Organization   | [26] 20.25                       | o          | o              | [26] 20.25                       | o          | o              |
| 14   | P-Access-Network-Info  | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c6             | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c7             |
| 15   | P-Charging-Function-Addresses  | [52] 4.5,<br>[52A] 4             | c10        | c11            | [52] 4.5,<br>[52A] 4             | c10        | c11            |
| 16   | P-Charging-Vector  | [52] 4.6,<br>[52A] 4             | c8         | c9             | [52] 4.6,<br>[52A] 4             | c8         | c9             |
| 18   | Privacy  | [33] 4.2                         | c4         | c4             | [33] 4.2                         | c4         | c4             |
| 19   | Require  | [26] 20.32                       | m          | m              | [26] 20.32                       | m          | m              |
| 20   | Server   | [26] 20.35                       | o          | o              | [26] 20.35                       | o          | o              |
| 20A  | Session-ID   | [162]                            | o          | c17            | [162]                            | o          | c17            |
| 21   | Timestamp  | [26] 20.38                       | m          | m              | [26] 20.38                       | c2         | c2             |
| 22   | To   | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 23   | User-Agent   | [26] 20.41                       | o          | o              | [26] 20.41                       | o          | o              |
| 24   | Via  | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 25   | Warning  | [26] 20.43                       | o          | o              | [26] 20.43                       | o          | o              |
| c1:  | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c2:  | IF A.4/6 THEN m ELSE n/a - - timestamping of requests.   |                                  |            |                |                                  |            |                |
| c4:  | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |                                  |            |                |                                  |            |                |
| c5:  | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.  |                                  |            |                |                                  |            |                |
| c6:  | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.   |                                  |            |                |                                  |            |                |
| c7:  | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller. |                                  |            |                |                                  |            |                |
| c8:  | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c9:  | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c10: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c11: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c12: | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).  |                                  |            |                |                                  |            |                |
| c14: | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.   |                                  |            |                |                                  |            |                |
| c17: | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.36: Supported header fields within the INFO response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Accept   | [26] 20.1  | o          | o              | [26] 20.1  | m          | m              |
| 2    | Accept-Encoding  | [26] 20.2  | o          | o              | [26] 20.2  | m          | m              |
| 3    | Accept-Language  | [26] 20.3  | o          | o              | [26] 20.3  | m          | m              |
| 4    | Accept-Resource-Priority   | [116] 3.2  | c5         | c5             | [116] 3.2  | c5         | c5             |
| 5    | Allow-Events   | [28] 7.2.2 | c3         | c3             | [28] 7.2.2 | c4         | c4             |
| 6    | Authentication-Info  | [26] 20.6  | c1         | c1             | [26] 20.6  | c2         | c2             |
| 9    | Supported  | [26] 20.37 | o          | o              | [26] 20.37 | m          | m              |
| c1:  | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c2:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c3:  | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.   |            |            |                |            |            |                |
| c4:  | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.   |            |            |                |            |            |                |
| c5:  | IF A.4/70A THEN m ELSE n/a - - inclusion of INFO, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol. |            |            |                |            |            |                |

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.37: Supported header fields within the INFO response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | o          | o              | [26] 20.18 | o          | o              |

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/103 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.37A: Void**

| Item | Header field | Ref. | RFC status | Profile status | Ref. | RFC status | Profile status |
|------|--------------|------|------------|----------------|------|------------|----------------|
|      |              |      |            |                |      |            |                |

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.38: Supported header fields within the INFO response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Proxy-Authenticate  | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 6    | WWW-Authenticate  | [26] 20.44 | m          | m              | [26] 20.44 | m          | m              |
| c1:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480 (Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.39: Supported header fields within the INFO response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | o              |

**Table A.40: Void**

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.41: Supported header fields within the INFO response**

| Item | Header field    | Sending  |            |                | Receiving |            |                |
|------|-----------------|--|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.   | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1  | o.1        | o.1            | [26] 20.1 | m          | m              |
| 2    | Accept-Encoding | [26] 20.2  | o.1        | o.1            | [26] 20.2 | m          | m              |
| 3    | Accept-Language | [26] 20.3  | o.1        | o.1            | [26] 20.3 | m          | m              |
| o.1  |                 | At least one of these capabilities is supported. |            |                |           |            |                |

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.41A: Supported header fields within the INFO response**

| Item | Header field             | Sending  |            |                | Receiving |            |                |
|------|--------------------------|--|------------|----------------|-----------|------------|----------------|
|      |                          | Ref.   | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority | [116] 3.2  | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  |                          | IF A.4/70A THEN m ELSE n/a - - inclusion of INFO, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol. |            |                |           |            |                |

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.42: Supported header fields within the INFO response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | m          | m              |

Prerequisite A.5/9B - - INFO response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.42A: Supported header fields within the INFO response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|---|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.  | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server | [48] 2  | x          | x              | [48] 2    | c1         | c1             |
| c1:  |                 | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |            |                |           |            |                |

Table A.43: Void

Table A.44: Void

Prerequisite A.5/9B - - INFO response

**Table A.45: Supported message bodies within the INFO response**

| Item | Header field | Sending |            |                | Receiving |            |                |
|------|--------------|---------|------------|----------------|-----------|------------|----------------|
|      |              | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |              |         |            |                |           |            |                |

#### A.2.1.4.7 INVITE method

Prerequisite A.5/8 - - INVITE request

**Table A.46: Supported header fields within the INVITE request**

| Item | Header field                  | Sending                |            |                | Receiving              |            |                |
|------|-------------------------------|------------------------|------------|----------------|------------------------|------------|----------------|
|      |                               | Ref.                   | RFC status | Profile status | Ref.                   | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1              | o          | c47            | [26] 20.1              | m          | m              |
| 1A   | Accept-Contact                | [56B] 9.2              | c24        | c24            | [56B] 9.2              | c32        | c32            |
| 2    | Accept-Encoding               | [26] 20.2              | o          | o              | [26] 20.2              | m          | m              |
| 3    | Accept-Language               | [26] 20.3              | o          | o              | [26] 20.3              | m          | m              |
| 4    | Alert-Info                    | [26] 20.4              | o          | o              | [26] 20.4              | c1         | c1             |
| 5    | Allow                         | [26] 20.5,<br>[26] 5.1 | o (note 1) | o              | [26] 20.5,<br>[26] 5.1 | m          | m              |
| 6    | Allow-Events                  | [28] 7.2.2             | c2         | c2             | [28] 7.2.2             | c53        | c53            |
| 7    | Answer-Mode                   | [158]                  | c49        | c49            | [158]                  | c50        | c50            |
| 8    | Authorization                 | [26] 20.7              | c3         | c3             | [26] 20.7              | c3         | c3             |
| 9    | Call-ID                       | [26] 20.8              | m          | m              | [26] 20.8              | m          | m              |
| 10   | Call-Info                     | [26] 20.9              | o          | o              | [26] 20.9              | o          | o              |
| 11   | Contact                       | [26] 20.10             | m          | m              | [26] 20.10             | m          | m              |
| 12   | Content-Disposition           | [26] 20.11             | o          | o              | [26] 20.11             | m          | m              |
| 13   | Content-Encoding              | [26] 20.12             | o          | o              | [26] 20.12             | m          | m              |
| 14   | Content-Language              | [26] 20.13             | o          | o              | [26] 20.13             | m          | m              |
| 15   | Content-Length                | [26] 20.14             | m          | m              | [26] 20.14             | m          | m              |
| 16   | Content-Type                  | [26] 20.15             | m          | m              | [26] 20.15             | m          | m              |
| 17   | CSeq                          | [26] 20.16             | m          | m              | [26] 20.16             | m          | m              |
| 18   | Date                          | [26] 20.17             | c4         | c4             | [26] 20.17             | m          | m              |
| 19   | Expires                       | [26] 20.19             | o          | o              | [26] 20.19             | o          | o              |
| 19A  | Feature-Caps                  | [190]                  | c59        | c59            | [190]                  | c58        | c58            |
| 20   | From                          | [26] 20.20             | m          | m              | [26] 20.20             | m          | m              |
| 20A  | Geolocation                   | [89] 4.1               | c33        | c33            | [89] 4.1               | c33        | c33            |
| 20B  | Geolocation-Routing           | [89] 4.2               | c33        | c33            | [89] 4.2               | c33        | c33            |
| 20C  | History-Info                  | [66] 4.1               | c31        | c31            | [66] 4.1               | c31        | c31            |
| 21   | In-Reply-To                   | [26] 20.21             | o          | o              | [26] 20.21             | o          | o              |
| 21A  | Join                          | [61] 7.1               | c30        | c30            | [61] 7.1               | c30        | c30            |
| 21B  | Max-Breadth                   | [117] 5.8              | n/a        | c45            | [117] 5.8              | c46        | c46            |
| 22   | Max-Forwards                  | [26] 20.22             | m          | m              | [26] 20.22             | n/a        | c52            |
| 23   | MIME-Version                  | [26] 20.24             | o          | o              | [26] 20.24             | m          | m              |
| 23A  | Min-SE                        | [58] 5                 | c26        | c26            | [58] 5                 | c25        | c25            |
| 24   | Organization                  | [26] 20.25             | o          | o              | [26] 20.25             | o          | o              |
| 24A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2   | c15        | c16            | [52] 4.4,<br>[234] 2   | c15        | c17            |
| 24B  | P-Asserted-Identity           | [34] 9.1               | n/a        | c65            | [34] 9.1               | c7         | c7             |
| 24C  | P-Asserted-Service            | [121] 4.1              | n/a        | c67            | [121] 4.1              | c38        | c38            |
| 24D  | P-Called-Party-ID             | [52] 4.2               | x          | x              | [52] 4.2               | c13        | c13            |
| 24E  | P-Charging-Function-Addresses | [52] 4.5               | c20        | c21            | [52] 4.5               | c20        | c21            |
| 24F  | P-Charging-Vector             | [52] 4.6               | c18        | c19            | [52] 4.6               | c18        | c19            |
| 24H  | P-Early-Media                 | [109] 8                | c34        | c34            | [109] 8                | c34        | c34            |
| 25   | P-Media-Authorization         | [31] 5.1               | n/a        | n/a            | [31] 5.1               | c11        | c12            |
| 25A  | P-Preferred-Identity          | [34] 9.2               | c7         | c5             | [34] 9.2               | n/a        | n/a            |
| 25B  | P-Preferred-Service           | [121] 4.2              | c37        | c36            | [121] 4.2              | n/a        | n/a            |
| 25C  | P-Private-Network-Indication  | [134]                  | c42        | c42            | [134]                  | c42        | c42            |
| 25D  | P-Profile-Key                 | [97] 5                 | n/a        | n/a            | [97] 5                 | n/a        | n/a            |
| 25E  | P-Served-User                 | [133] 6                | c51        | c51            | [133] 6                | c51        | c51            |
| 25F  | P-User-Database               | [82] 4                 | n/a        | n/a            | [82] 4                 | n/a        | n/a            |
| 25G  | P-Visited-Network-ID          | [52] 4.3               | x (note 3) | x              | [52] 4.3               | c14        | n/a            |
| 26   | Priority                      | [26] 20.26             | o          | o              | [26] 20.26             | o          | o              |
| 26A  | Privacy                       | [33] 4.2               | c9         | c9             | [33] 4.2               | c9         | c9             |
| 26B  | Priv-Answer-Mode              | [158]                  | c49        | c49            | [158]                  | c50        | c50            |
| 27   | Proxy-Authorization           | [26] 20.28             | c6         | c6             | [26] 20.28             | n/a        | n/a            |
| 28   | Proxy-Require                 | [26] 20.29             | o (note 2) | o (note 2)     | [26] 20.29             | n/a        | n/a            |
| 28A  | Reason                        | [34A] 2                | c8         | c8             | [34A] 2                | c8         | c55            |
| 29   | Record-Route                  | [26] 20.30             | n/a        | c52            | [26] 20.30             | m          | m              |
| 29A  | Recv-Info                     | [25] 5.2.3             | c48        | c48            | [25] 5.2.3             | c48        | c48            |
| 30   | Referred-By                   | [59] 3                 | c27        | c27            | [59] 3                 | c28        | c28            |
| 31   | Reject-Contact                | [56B] 9.2              | c24        | c24            | [56B] 9.2              | c32        | c32            |
| 31A  | Replaces                      | [60] 6.1               | c29        | c29            | [60] 6.1               | c29        | c29            |
| 31B  | Reply-To                      | [26] 20.31             | o          | o              | [26] 20.31             | o          | o              |

| Item | Header field        | Sending         |            |                | Receiving       |            |                |
|------|---------------------|-----------------|------------|----------------|-----------------|------------|----------------|
|      |                     | Ref.            | RFC status | Profile status | Ref.            | RFC status | Profile status |
| 31C  | Request-Disposition | [56B] 9.1       | c24        | c24            | [56B] 9.1       | c32        | c32            |
| 32   | Require             | [26] 20.32      | m          | m              | [26] 20.32      | m          | m              |
| 32A  | Resource-Priority   | [116] 3.1       | c35        | c35            | [116] 3.1       | c35        | c35            |
| 33   | Route               | [26] 20.34      | m          | m              | [26] 20.34      | n/a        | c52            |
| 33A  | Security-Client     | [48] 2.3.1      | c22        | c22            | [48] 2.3.1      | n/a        | n/a            |
| 33B  | Security-Verify     | [48] 2.3.1      | c23        | c23            | [48] 2.3.1      | n/a        | n/a            |
| 33D  | Session-Expires     | [58] 4          | c25        | c25            | [58] 4          | c25        | c25            |
| 33E  | Session-ID          | [162]           | o          | c54            | [162]           | o          | c54            |
| 34   | Subject             | [26] 20.36      | o          | o              | [26] 20.36      | o          | o              |
| 35   | Supported           | [26] 20.37      | m          | m              | [26] 20.37      | m          | m              |
| 35A  | Target-Dialog       | [184] 7         | c56        | c56            | [xxa] 7         | c57        | c57            |
| 36   | Timestamp           | [26] 20.38      | c10        | c10            | [26] 20.38      | m          | m              |
| 37   | To                  | [26] 20.39      | m          | m              | [26] 20.39      | m          | m              |
| 37A  | Trigger-Consent     | [125]<br>5.11.2 | c39        | c39            | [125]<br>5.11.2 | c40        | c40            |
| 38   | User-Agent          | [26] 20.41      | o          | o              | [26] 20.41      | o          | o              |
| 38A  | User-to-User        | [126] 7         | c41        | c41            | [126] 7         | c41        | c41            |
| 39   | Via                 | [26] 20.42      | m          | m              | [26] 20.42      | m          | m              |

| Item | Header field   | Sending |            |                | Receiving |            |   |
|------|--|---------|------------|----------------|-----------|------------|---|
|      |  | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status  |
| c1:  | IF A.4/12 THEN m ELSE n/a  |         |            |                |           |            | -- downloading of alerting information.   |
| c2:  | IF A.4/22 THEN m ELSE n/a  |         |            |                |           |            | -- acting as the notifier of event information.   |
| c3:  | IF A.4/7 THEN m ELSE n/a   |         |            |                |           |            | -- authentication between UA and UA.  |
| c4:  | IF A.4/11 THEN o ELSE n/a  |         |            |                |           |            | -- insertion of date in requests and responses.   |
| c5:  | IF A.3/1 AND A.4/25 THEN o ELSE n/a  |         |            |                |           |            | -- UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c6:  | IF A.4/8A THEN m ELSE n/a  |         |            |                |           |            | -- authentication between UA and proxy.   |
| c7:  | IF A.4/25 THEN o ELSE n/a  |         |            |                |           |            | -- private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.   |
| c8:  | IF A.4/38 THEN o ELSE n/a  |         |            |                |           |            | -- the Reason header field for the session initiation protocol.   |
| c9:  | IF A.4/26 THEN o ELSE n/a  |         |            |                |           |            | -- a privacy mechanism for the Session Initiation Protocol (SIP).   |
| c10: | IF A.4/6 THEN o ELSE n/a   |         |            |                |           |            | -- timestamping of requests.  |
| c11: | IF A.4/19 THEN m ELSE n/a  |         |            |                |           |            | -- SIP extensions for media authorization.  |
| c12: | IF A.3/1 AND A.4/19 THEN m ELSE n/a  |         |            |                |           |            | -- UE, SIP extensions for media authorization.  |
| c13: | IF A.4/32 THEN o ELSE n/a  |         |            |                |           |            | -- the P-Called-Party-ID extension.   |
| c14: | IF A.4/33 THEN o ELSE n/a  |         |            |                |           |            | -- the P-Visited-Network-ID extension.  |
| c15: | IF A.4/34 THEN o ELSE n/a  |         |            |                |           |            | -- the P-Access-Network-Info header extension.  |
| c16: | IF A.4/34 AND (A.3/1 OR A.3/2A OR A.3/7 OR A.3A/81) THEN m ELSE n/a  |         |            |                |           |            | -- the P-Access-Network-Info header extension and UE, P-CSCF (IMS-ALG), the AS or the MSC server enhanced for ICS.  |
| c17: | IF A.4/34 AND (A.3/2A OR A.3A/81 OR A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a                            |         |            |                |           |            | -- the P-Access-Network-Info header extension and P-CSCF (IMS-ALG), the MSC server enhanced for ICS, AS acting as terminating UA, AS acting as third-party call controller or EATF.   |
| c18: | IF A.4/36 THEN o ELSE n/a  |         |            |                |           |            | -- the P-Charging-Vector header extension.  |
| c19: | IF A.4/36 THEN m ELSE n/a  |         |            |                |           |            | -- the P-Charging-Vector header extension.  |
| c20: | IF A.4/35 THEN o ELSE n/a  |         |            |                |           |            | -- the P-Charging-Function-Addresses header extension.  |
| c21: | IF A.4/35 THEN m ELSE n/a  |         |            |                |           |            | -- the P-Charging-Function-Addresses header extension.  |
| c22: | IF A.4/37 OR A.4/37A THEN o ELSE n/a   |         |            |                |           |            | -- security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 4).   |
| c23: | IF A.4/37 OR A.4/37A THEN m ELSE n/a   |         |            |                |           |            | -- security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |
| c24: | IF A.4/40 THEN o ELSE n/a  |         |            |                |           |            | -- caller preferences for the session initiation protocol.  |
| c25: | IF A.4/42 THEN m ELSE n/a  |         |            |                |           |            | -- the SIP session timer.   |
| c26: | IF A.4/42 THEN o ELSE n/a  |         |            |                |           |            | -- the SIP session timer.   |
| c27: | IF A.4/43 THEN m ELSE n/a  |         |            |                |           |            | -- the SIP Referred-By mechanism.   |
| c28: | IF A.4/43 THEN o ELSE n/a  |         |            |                |           |            | -- the SIP Referred-By mechanism.   |
| c29: | IF A.4/44 THEN m ELSE n/a  |         |            |                |           |            | -- the Session Initiation Protocol (SIP) "Replaces" header.   |
| c30: | IF A.4/45 THEN m ELSE n/a  |         |            |                |           |            | -- the Session Initiation Protocol (SIP) "Join" header.   |
| c31: | IF A.4/47 THEN m ELSE n/a  |         |            |                |           |            | -- an extension to the session initiation protocol for request history information.   |
| c32: | IF A.4/40 THEN m ELSE n/a  |         |            |                |           |            | -- caller preferences for the session initiation protocol.  |
| c33: | IF A.4/60 THEN m ELSE n/a  |         |            |                |           |            | -- SIP location conveyance.   |
| c34: | IF A.4/66 THEN m ELSE n/a  |         |            |                |           |            | -- The SIP P-Early-Media private header extension for authorization of early media.   |
| c35: | IF A.4/70 THEN m ELSE n/a  |         |            |                |           |            | -- communications resource priority for the session initiation protocol.  |
| c36: | IF (A.3/1 OR A.3A/81) AND A.4/74 THEN o ELSE n/a   |         |            |                |           |            | -- UE, MSC Server enhanced for ICS and SIP extension for the identification of services.  |
| c37: | IF A.4/74 THEN o ELSE n/a  |         |            |                |           |            | -- SIP extension for the identification of services.  |
| c38: | IF A.4/74 THEN m ELSE n/a  |         |            |                |           |            | -- SIP extension for the identification of services.  |
| c39: | IF A.4/75A THEN m ELSE n/a   |         |            |                |           |            | -- a relay within the framework for consent-based communications in SIP.  |
| c40: | IF A.4/75B THEN m ELSE n/a   |         |            |                |           |            | -- a recipient within the framework for consent-based communications in SIP.  |
| c41: | IF A.4/76 THEN o ELSE n/a  |         |            |                |           |            | -- transporting user to user information for call centers using SIP.  |
| c42: | IF A.4/77 THEN m ELSE n/a  |         |            |                |           |            | -- the SIP P-Private-Network-Indication private-header (P-Header).  |
| c45: | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o |         |            |                |           |            | -- addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network. |
| c46: | IF A.4/71 THEN m ELSE n/a  |         |            |                |           |            | -- addressing an amplification vulnerability in session initiation protocol forking proxies.  |
| c47: | IF A.3/1 AND A.4/2B THEN m ELSE o  |         |            |                |           |            | -- UE and initiating a session.   |
| c48: | IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a   |         |            |                |           |            | -- SIP INFO method and package framework, legacy INFO usage.  |



| Item  | Header field  | Sending |            |                | Receiving |            |                |
|---|---|---------|------------|----------------|-----------|------------|----------------|
|   |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| c49:  | IF A.4/87 THEN o ELSE n/a - - requesting answering modes for SIP.   |         |            |                |           |            |                |
| c50:  | IF A.4/87 THEN m ELSE n/a - - requesting answering modes for SIP.   |         |            |                |           |            |                |
| c51:  | IF A.4/78 THEN m ELSE n/a - - the SIP P-Served-User private header.   |         |            |                |           |            |                |
| c52:  | IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.  |         |            |                |           |            |                |
| c53:  | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.  |         |            |                |           |            |                |
| c54:  | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.  |         |            |                |           |            |                |
| c55:  | IF A.4/38 THEN IF A.3A/83 THEN m ELSE o ELSE n/a - - the Reason header field for the session initiation protocol, SCC application server.   |         |            |                |           |            |                |
| c56:  | IF A.4/99 THEN o ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.   |         |            |                |           |            |                |
| c57:  | IF A.4/99 THEN m ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.   |         |            |                |           |            |                |
| c58:  | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.   |         |            |                |           |            |                |
| c59:  | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.  |         |            |                |           |            |                |
| c65:  | IF A.4/25 AND (A.3/6 OR A.3/7B OR A.3/8 A.3/81 OR OR A.3A/83 OR A.3A/89) THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and MGCF, AS acting as originating UA, MRFC, MSC Server enhanced for ICS, SCC application server, ATCF (UA). |         |            |                |           |            |                |
| c67:  | IF A.4/74 AND A.3/7B THEN o ELSE n/a - - SIP extension for the identification of services and AS acting as originating UA.  |         |            |                |           |            |                |
| o.1:  | At least one of these shall be supported.   |         |            |                |           |            |                |
| NOTE 1: RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.   |   |         |            |                |           |            |                |
| NOTE 2: No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.         |   |         |            |                |           |            |                |
| NOTE 3: The strength of this requirement in RFC 7315 [52] is SHOULD NOT, rather than MUST NOT.  |   |         |            |                |           |            |                |
| NOTE 4: Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19]. |   |         |            |                |           |            |                |

Prerequisite A.5/8 - - INVITE request

**Table A.47: Supported message bodies within the INVITE request**

| Item | Header  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | XML Schema for PSTN   | [11B]   |            | c1             | [11B]     |            | c1             |
| 2    | application/vnd.3gpp.ussd   | [8W]    |            | c2             | [8W]      |            | c3             |
| c1:  | IF A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9B OR A.3/13B THEN o ELSE n/a - - MGCF, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, IBCF (IMS-ALG), ISC gateway function (IMS-ALG). |         |            |                |           |            |                |
| c2:  | IF A.3A/92 OR A.3/9 OR A.3/2 OR A.3A/89 THEN m ELSE n/a - - USSI UE, IBCF, P-CSCF, ATCF (UA).   |         |            |                |           |            |                |
| c3:  | IF A.3A/93 OR A.3/9 OR A.3/2 OR A.3A/89 THEN m ELSE n/a - - USSI AS, IBCF, P-CSCF, ATCF (UA).   |         |            |                |           |            |                |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/1 - - Additional for 100 (Trying) response

**Table A.48: Supported header fields within the INVITE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID  | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length   | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq   | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date   | [26] 20.17 | c1         | c1             | [26] 20.17 | m          | m              |
| 5    | From   | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To   | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via  | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |            |            |                |            |            |                |

Prerequisite A.5/9 - - INVITE response for all remaining status-codes

**Table A.49: Supported header fields within the INVITE response**

| Item           | Header field   | Sending                          |            |                | Receiving                        |            |                |
|----------------|--|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|                |  | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A             | Allow  | [26] 20.5                        | c12        | c12            | [26] 20.5                        | m          | m              |
| 1              | Call-ID  | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 1A             | Call-Info  | [26] 20.9                        | o          | o              | [26] 20.9                        | o          | o              |
| 2              | Content-Disposition  | [26] 20.11                       | o          | o              | [26] 20.11                       | m          | m              |
| 3              | Content-Encoding   | [26] 20.12                       | o          | o              | [26] 20.12                       | m          | m              |
| 4              | Content-Language   | [26] 20.13                       | o          | o              | [26] 20.13                       | m          | m              |
| 5              | Content-Length   | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6              | Content-Type   | [26] 20.15                       | m          | m              | [26] 20.15                       | m          | m              |
| 7              | CSeq   | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8              | Date   | [26] 20.17                       | c1         | c1             | [26] 20.17                       | m          | m              |
| 8 <sup>a</sup> | Expires  | [26] 20.19                       | o          | o              | [26] 20.19                       | o          | o              |
| 9              | From   | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A             | Geolocation-Error  | [89] 4.3                         | c14        | c14            | [89] 4.3                         | c14        | c14            |
| 9B             | History-Info   | [66] 4.1                         | c13        | c13            | [66] 4.1                         | c13        | c13            |
| 10             | MIME-Version   | [26] 20.24                       | o          | o              | [26] 20.24                       | m          | m              |
| 11             | Organization   | [26] 20.25                       | o          | o              | [26] 20.25                       | o          | o              |
| 11A            | P-Access-Network-Info  | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c6             | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c7             |
| 11B            | P-Asserted-Identity  | [34] 9.1                         | n/a        | c22            | [34] 9.1                         | c3         | c3             |
| 11C            | P-Charging-Function-Addresses  | [52] 4.5,<br>[52A] 4             | c10        | c11            | [52] 4.5,<br>[52A] 4             | c11        | c11            |
| 11D            | P-Charging-Vector  | [52] 4.6,<br>[52A] 4             | c8         | c9             | [52] 4.6,<br>[52A] 4             | c8         | c9             |
| 11F            | P-Preferred-Identity   | [34] 9.2                         | c3         | x              | [34] 9.2                         | n/a        | n/a            |
| 11G            | Privacy  | [33] 4.2                         | c4         | c4             | [33] 4.2                         | c4         | c4             |
| 11H            | Reply-To   | [26] 20.31                       | o          | o              | [26] 20.31                       | o          | o              |
| 11I            | Require  | [26] 20.32                       | m          | m              | [26] 20.32                       | m          | m              |
| 11J            | Server   | [26] 20.35                       | o          | o              | [26] 20.35                       | o          | o              |
| 11K            | Session-ID   | [162]                            | o          | c18            | [162]                            | o          | c18            |
| 12             | Timestamp  | [26] 20.38                       | m          | m              | [26] 20.38                       | c2         | c2             |
| 13             | To   | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 13A            | User-Agent   | [26] 20.41                       | o          | o              | [26] 20.41                       | o          | o              |
| 13B            | User-to-User   | [126] 7                          | c15        | c15            | [126] 7                          | c15        | c15            |
| 14             | Via  | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 15             | Warning  | [26] 20.43                       | o (note)   | o              | [26] 20.43                       | o          | o              |
| c1:            | IF A.4/11 THEN o ELSE n/a -- insertion of date in requests and responses.  |                                  |            |                |                                  |            |                |
| c2:            | IF A.4/6 THEN m ELSE n/a -- timestamping of requests.  |                                  |            |                |                                  |            |                |
| c3:            | IF A.4/25 THEN o ELSE n/a -- private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |                                  |            |                |                                  |            |                |
| c4:            | IF A.4/26 THEN o ELSE n/a -- a privacy mechanism for the Session Initiation Protocol (SIP).  |                                  |            |                |                                  |            |                |
| c5:            | IF A.4/34 THEN o ELSE n/a -- the P-Access-Network-Info header extension.   |                                  |            |                |                                  |            |                |
| c6:            | IF A.4/34 AND (A.3/1 OR A.3/2A OR A.3/7 OR A.3A/81) THEN m ELSE n/a -- the P-Access-Network-Info header extension and UE, P-CSCF (IMS-ALG), AS or MSC server enhanced for ICS.   |                                  |            |                |                                  |            |                |
| c7:            | IF A.4/34 AND (A.3/2A OR A.3A/81 OR A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a -- the P-Access-Network-Info header extension and P-CSCF (IMS-ALG), MSC server enhanced for ICS, AS acting as terminating UA, AS acting as third-party call controller or EATF.  |                                  |            |                |                                  |            |                |
| c8:            | IF A.4/36 THEN o ELSE n/a -- the P-Charging-Vector header extension.   |                                  |            |                |                                  |            |                |
| c9:            | IF A.4/36 THEN m ELSE n/a -- the P-Charging-Vector header extension.   |                                  |            |                |                                  |            |                |
| c10:           | IF A.4/35 THEN o ELSE n/a -- the P-Charging-Function-Addresses header extension.   |                                  |            |                |                                  |            |                |
| c11:           | IF A.4/35 THEN m ELSE n/a -- the P-Charging-Function-Addresses header extension.   |                                  |            |                |                                  |            |                |
| c12:           | IF A.6/6 OR A.6/18 THEN m ELSE o -- 200 (OK), 405 (Method Not Allowed).  |                                  |            |                |                                  |            |                |
| c13:           | IF A.4/47 THEN m ELSE n/a -- an extension to the session initiation protocol for request history information.  |                                  |            |                |                                  |            |                |
| c14:           | IF A.4/60 THEN m ELSE n/a -- SIP location conveyance.  |                                  |            |                |                                  |            |                |
| c15:           | IF A.4/76 THEN o ELSE n/a -- transporting user to user information for call centers using SIP.   |                                  |            |                |                                  |            |                |
| c18:           | IF A.4/91 THEN m ELSE n/a -- the Session-ID header.  |                                  |            |                |                                  |            |                |
| c22:           | IF A.4/25 AND (A.3/6 OR A.3/7B OR A.3/8 OR A.3A/81 OR OR A.3A/83 OR A.3A/89) THEN o ELSE n/a -- private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and MGCF, AS acting as originating UA, MRFC, MSC Server enhanced for ICS, SCC application server, ATCF (UA). |                                  |            |                |                                  |            |                |
| NOTE:          | For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.  |                                  |            |                |                                  |            |                |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/101A - - Additional for 18x response

**Table A.50: Supported header fields within the INVITE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Contact  | [26] 20.10 | o          | m              | [26] 20.10 | m          | m              |
| 4A   | Feature-Caps   | [190]      | c17        | c17            | [190]      | c16        | c16            |
| 5    | P-Answer-State   | [111]      | c13        | c13            | [111]      | c13        | c13            |
| 5A   | P-Early-Media  | [109] 8    | c14        | c14            | [109] 8    | c14        | c14            |
| 6    | P-Media-Authorization  | [31] 5.1   | n/a        | n/a            | [31] 5.1   | c11        | c12            |
| 6A   | Reason   | [130]      | o          | c15            | [130]      | o          | c15            |
| 7    | Record-Route   | [26] 20.30 | o          | m              | [26] 20.30 | m          | m              |
| 8    | Recv-Info  | [25] 5.2.3 | c4         | c4             | [25] 5.2.3 | c4         | c4             |
| 9    | RSeq   | [27] 7.1   | c2         | m              | [27] 7.1   | c3         | m              |
| c2:  | IF A.4/14 THEN o ELSE n/a - - reliability of provisional responses in SIP.   |            |            |                |            |            |                |
| c3:  | IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses in SIP.   |            |            |                |            |            |                |
| c4:  | IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.   |            |            |                |            |            |                |
| c11: | IF A.4/19 THEN m ELSE n/a - - SIP extensions for media authorization.  |            |            |                |            |            |                |
| c12: | IF A.3/1 AND A.4/19 THEN m ELSE n/a - - UE, SIP extensions for media authorization.  |            |            |                |            |            |                |
| c13: | IF A.4/65 THEN m ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular.                                |            |            |                |            |            |                |
| c14: | IF A.4/66 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.   |            |            |                |            |            |                |
| c15: | IF A.4/38A THEN o ELSE n/a - - use of the Reason header field in Session Initiation Protocol (SIP) responses.  |            |            |                |            |            |                |
| c16: | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.  |            |            |                |            |            |                |
| c17: | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network. |            |            |                |            |            |                |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/2 - - Additional for 180 (Ringing) response

**Table A.50A: Supported header fields within the INVITE response**

| Item   | Header field | Sending   |            |                | Receiving |            |                |
|--|--------------|-----------|------------|----------------|-----------|------------|----------------|
|  |              | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1  | Alert-Info   | [26] 20.4 | o          | c1             | [26] 20.4 | o          | c1             |
| c1: IF A.4/96 THEN m ELSE o - - Alert-Info URNs for the Session Initiation Protocol. |              |           |            |                |           |            |                |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/5A - - Additional for 199 (Early Dialog Terminated) response

**Table A.50B: Supported header fields within the INVITE response**

| Item   | Header field | Sending    |            |                | Receiving  |            |                |
|--|--------------|------------|------------|----------------|------------|------------|----------------|
|  |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4  | Contact      | [26] 20.10 | o          | m              | [26] 20.10 | m          | m              |
| 5  | Reason       | [130]      | o          | c5             | [130]      | o          | c5             |
| 7  | Record-Route | [26] 20.30 | o          | m              | [26] 20.30 | m          | m              |
| 8  | Recv-Info    | [25] 5.2.3 | c4         | c4             | [25] 5.2.3 | c4         | c4             |
| 9  | RSeq         | [27] 7.1   | c2         | m              | [27] 7.1   | c3         | m              |
| c2: IF A.4/14 THEN o ELSE n/a - - reliability of provisional responses in SIP.                                     |              |            |            |                |            |            |                |
| c3: IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses in SIP.                                     |              |            |            |                |            |            |                |
| c4: IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage. |              |            |            |                |            |            |                |
| C5: IF A.4/38A THEN o ELSE n/a - - use of the Reason header field in Session Initiation Protocol (SIP) responses?  |              |            |            |                |            |            |                |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.51: Supported header fields within the INVITE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Accept   | [26] 20.1  | o          | o              | [26] 20.1  | m          | m              |
| 1A   | Accept-Encoding  | [26] 20.2  | o          | o              | [26] 20.2  | m          | m              |
| 1B   | Accept-Language  | [26] 20.3  | o          | o              | [26] 20.3  | m          | m              |
| 1C   | Accept-Resource-Priority   | [116] 3.2  | c15        | c15            | [116] 3.2  | c15        | c15            |
| 2    | Allow-Events   | [28] 7.2.2 | c3         | c3             | [28] 7.2.2 | c4         | c4             |
| 3    | Answer-Mode  | [158]      | c6         | c6             | [158]      | c7         | c7             |
| 4    | Authentication-Info  | [26] 20.6  | c1         | c1             | [26] 20.6  | c2         | c2             |
| 6    | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | m          | m              |
| 6A   | Feature-Caps   | [190]      | c18        | c18            | [190]      | c17        | c17            |
| 7    | P-Answer-State   | [111]      | c14        | c14            | [111]      | c14        | c14            |
| 8    | P-Media-Authorization  | [31] 5.1   | n/a        | n/a            | [31] 5.1   | c11        | c12            |
| 8A   | Priv-Answer-Mode   | [158]      | c6         | c6             | [158]      | c7         | c7             |
| 9    | Record-Route   | [26] 20.30 | m          | m              | [26] 20.30 | m          | m              |
| 9A   | Recv-Info  | [25] 5.2.3 | c5         | c5             | [25] 5.2.3 | c5         | c5             |
| 10   | Session-Expires  | [58] 4     | c13        | c13            | [58] 4     | c13        | c13            |
| 13   | Supported  | [26] 20.37 | m          | m              | [26] 20.37 | m          | m              |
| c1:  | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c2:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c3:  | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.   |            |            |                |            |            |                |
| c4:  | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.   |            |            |                |            |            |                |
| c5:  | IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.   |            |            |                |            |            |                |
| c6   | IF A.4/87 THEN o ELSE n/a - - requesting answering modes for SIP.  |            |            |                |            |            |                |
| c7   | IF A.4/87 THEN m ELSE n/a - - requesting answering modes for SIP.  |            |            |                |            |            |                |
| c11: | IF A.4/19 THEN m ELSE n/a - - SIP extensions for media authorization.  |            |            |                |            |            |                |
| c12: | IF A.3/1 AND A.4/19 THEN m ELSE n/a - - UE, SIP extensions for media authorization.  |            |            |                |            |            |                |
| c13: | IF A.4/42 THEN m ELSE n/a - - the SIP session timer.   |            |            |                |            |            |                |
| c14: | IF A.4/65 THEN m ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular.                                |            |            |                |            |            |                |
| c15: | IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.  |            |            |                |            |            |                |
| c17: | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.  |            |            |                |            |            |                |
| c18: | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network. |            |            |                |            |            |                |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.51A: Supported header fields within the INVITE response**

| Item  | Header field | Sending    |            |                | Receiving  |            |                |
|---|--------------|------------|------------|----------------|------------|------------|----------------|
|   |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1   | Error-Info   | [26] 20.18 | o          | o              | [26] 20.18 | o          | o              |
| 2   | Reason       | [130]      | o          | c1             | [130]      | o          | c1             |
| c1: IF A.4/38A THEN o ELSE n/a - - use of the Reason header field in Session Initiation Protocol (SIP) responses? |              |            |            |                |            |            |                |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.52: Supported header fields within the INVITE response**

| Item  | Header field | Sending    |            |                | Receiving  |            |                |
|---|--------------|------------|------------|----------------|------------|------------|----------------|
|   |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4   | Contact      | [26] 20.10 | o (note 1) | o              | [26] 20.10 | m          | m              |
| NOTE: The strength of this requirement is RECOMMENDED rather than OPTIONAL. |              |            |            |                |            |            |                |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.53: Supported header fields within the INVITE response**

| Item   | Header field       | Sending    |            |                | Receiving  |            |                |
|--|--------------------|------------|------------|----------------|------------|------------|----------------|
|  |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 6  | Proxy-Authenticate | [26] 20.27 | c3         | c3             | [26] 20.27 | c3         | c3             |
| 13   | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | m          | m              |
| c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |                    |            |            |                |            |            |                |
| c2: IF A.4/6 THEN m ELSE n/a - - timestamping of requests.                     |                    |            |            |                |            |            |                |
| c3: IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.  |                    |            |            |                |            |            |                |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/16 - - Additional for 403 (Forbidden) response

**Table A.53A: Supported header fields within the INVITE response**

| Item  | Header field       | Sending |            |                | Receiving |            |                |
|---|--------------------|---------|------------|----------------|-----------|------------|----------------|
|   |                    | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1   | P-Refused-URI-List | [183]   | c1         | c1             | [183]     | c1         | c1             |
| c1: IF A.4/98 THEN m ELSE n/a -- The SIP P-Refused-URI-List private-header. |                    |         |            |                |           |            |                |



Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 600 (Busy Everywhere), 603 (Decline) response

**Table A.54: Supported header fields within the INVITE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 8    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | o              |

**Table A.55: Void**

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.56: Supported header fields within the INVITE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 6    | Proxy-Authenticate  | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 11   | WWW-Authenticate  | [26] 20.44 | o          | o              | [26] 20.44 | o          | o              |
| c1:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.57: Supported header fields within the INVITE response**

| Item | Header field                                     | Sending   |            |                | Receiving |            |                |
|------|--|-----------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept   | [26] 20.1 | o.1        | o.1            | [26] 20.1 | m          | m              |
| 2    | Accept-Encoding                                  | [26] 20.2 | o.1        | o.1            | [26] 20.2 | m          | m              |
| 3    | Accept-Language                                  | [26] 20.3 | o.1        | o.1            | [26] 20.3 | m          | m              |
| o.1  | At least one of these capabilities is supported. |           |            |                |           |            |                |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.57A: Supported header fields within the INVITE response**

| Item  | Header field             | Sending   |            |                | Receiving |            |                |
|---|--------------------------|-----------|------------|----------------|-----------|------------|----------------|
|   |                          | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1   | Accept-Resource-Priority | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1: IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol. |                          |           |            |                |           |            |                |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.58: Supported header fields within the INVITE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 10   | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | m          | m              |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.58A: Supported header fields within the INVITE response**

| Item  | Header field    | Sending |            |                | Receiving |            |                |
|---|-----------------|---------|------------|----------------|-----------|------------|----------------|
|   |                 | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3   | Security-Server | [48] 2  | x          | x              | [48] 2    | c1         | c1             |
| c1: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |                 |         |            |                |           |            |                |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/28A - - Additional for 422 (Session Interval Too Small) response

**Table A.58B: Supported header fields within the INVITE response**

| Item | Header field | Sending  |            |                | Receiving |            |                |
|------|--------------|--|------------|----------------|-----------|------------|----------------|
|      |              | Ref.   | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Min-SE       | [58] 5   | c1         | c1             | [58] 5    | c1         | c1             |
| c1:  |              | IF A.4/42 THEN o ELSE n/a - - the SIP session timer. |            |                |           |            |                |

**Table A.59: Void**

**Table A.60: Void**

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/29H - - Additional for 470 (Consent Needed) response

**Table A.60A: Supported header fields within the INVITE response**

| Item | Header field       | Sending     |            |                | Receiving   |            |                |
|------|--------------------|-------------|------------|----------------|-------------|------------|----------------|
|      |                    | Ref.        | RFC status | Profile status | Ref.        | RFC status | Profile status |
| 1    | Permission-Missing | [125] 5.9.3 | m          | m              | [125] 5.9.3 | m          | m              |

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/45 - - 503 (Service Unavailable)

**Table A.61: Supported header fields within the INVITE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 8    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | m              |

**Table A.61A: Void**

Prerequisite A.5/9 - - INVITE response

**Table A.62: Supported message bodies within the INVITE response**

| Item | Header                        | Sending  |            |                | Receiving     |            |                |
|------|-------------------------------|--|------------|----------------|---------------|------------|----------------|
|      |                               | Ref.   | RFC status | Profile status | Ref.          | RFC status | Profile status |
| 1    | XML Schema for PSTN           | [11B]  |            | c1             | [11B]         |            | c1             |
| 2    | Recipient list                | [183]  | c2         | c2             | [183]         | c2         | c2             |
| 3    | 3GPP IM CN subsystem XML body | subclause 7.6  | n/a        | c3             | subclause 7.6 | n/a        | c4 (note)      |
| c1:  |                               | IF A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9B OR A.3/13B THEN o ELSE n/a - - MGCF, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, IBCF (IMS-ALG), ISC gateway function (IMS-ALG).  |            |                |               |            |                |
| c2:  |                               | IF A.3/9B OR A.3/13B THEN m ELSE IF A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), ISC gateway function (IMS-ALG), AS acting as terminating UA, AS acting as originating UA, AS performing 3 <sup>rd</sup> party call control.   |            |                |               |            |                |
| c3:  |                               | IF A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C OR (A.4/103 AND A.3/2) OR (A.4/103 AND A.3/4) THEN m ELSE n/a - - IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), S-CSCF restoration procedures, P-CSCF, S-CSCF. |            |                |               |            |                |
| c4:  |                               | IF A.3/1 OR A.3/2 OR A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C THEN m ELSE IF A.3/4 THEN o ELSE n/a - - UE, P-CSCF, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), S-CSCF.   |            |                |               |            |                |

NOTE: If a IBCF (IMS-ALG) or a IBCF (Screening of SIP signalling) is unable to receive a 3GPP IM CN subsystem XML body from a S-CSCF in a serving network then the IBCF (IMS-ALG) or the IBCF (Screening of SIP signalling) support can be "o" instead of "m". Examples include an S-CSCF supporting S-CSCF restoration procedures.

## A.2.1.4.7A MESSAGE method

Prerequisite A.5/9A - - MESSAGE request

**Table A.62A: Supported header fields within the MESSAGE request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept-Contact                | [56B] 9.2            | c24        | c24            | [56B] 9.2            | c28        | c28            |
| 1A   | Allow                         | [26] 20.5            | o          | o              | [26] 20.5            | m          | m              |
| 2    | Allow-Events                  | [28] 7.2.2           | c1         | c1             | [28] 7.2.2           | c2         | c2             |
| 3    | Authorization                 | [26] 20.7            | c3         | c3             | [26] 20.7            | c3         | c3             |
| 4    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 5    | Call-Info                     | [26] 20.9            | o          | o              | [26] 20.9            | o          | o              |
| 6    | Content-Disposition           | [26] 20.11           | o          | o              | [26] 20.11           | m          | m              |
| 7    | Content-Encoding              | [26] 20.12           | o          | o              | [26] 20.12           | m          | m              |
| 8    | Content-Language              | [26] 20.13           | o          | o              | [26] 20.13           | m          | m              |
| 9    | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 10   | Content-Type                  | [26] 20.15           | m          | m              | [26] 29.15           | m          | m              |
| 11   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 12   | Date                          | [26] 20.17           | c4         | c4             | [26] 20.17           | m          | m              |
| 13   | Expires                       | [26] 20.19           | o          | o              | [26] 20.19           | o          | o              |
| 13A  | Feature-Caps                  | [190]                | c45        | c45            | [190]                | c44        | c44            |
| 14   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 14A  | Geolocation                   | [89] 4.1             | c29        | c29            | [89] 4.1             | c29        | c29            |
| 14B  | Geolocation-Routing           | [89] 4.2             | c29        | c29            | [89] 4.2             | c29        | c29            |
| 14C  | History-Info                  | [66] 4.1             | c27        | c27            | [66] 4.1             | c27        | c27            |
| 15   | In-Reply-To                   | [26] 20.21           | o          | o              | [26] 20.21           | o          | o              |
| 15A  | Max-Breadth                   | [117] 5.8            | n/a        | c39            | [117] 5.8            | c40        | c40            |
| 16   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | n/a        | c42            |
| 17   | MIME-Version                  | [26] 20.24           | o          | o              | [26] 20.24           | m          | m              |
| 18   | Organization                  | [26] 20.25           | o          | o              | [26] 20.25           | o          | o              |
| 18A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c15        | c16            | [52] 4.4,<br>[234] 2 | c15        | c16            |
| 18B  | P-Asserted-Identity           | [34] 9.1             | n/a        | c49            | [34] 9.1             | c11        | c11            |
| 18C  | P-Asserted-Service            | [121] 4.1            | n/a        | c50            | [121] 4.1            | c33        | c33            |
| 18D  | P-Called-Party-ID             | [52] 4.2             | x          | x              | [52] 4.2             | c13        | c13            |
| 18E  | P-Charging-Function-Addresses | [52] 4.5             | c20        | c21            | [52] 4.5             | c20        | c21            |
| 18F  | P-Charging-Vector             | [52] 4.6             | c18        | c19            | [52] 4.6             | c18        | c19            |
| 18H  | P-Preferred-Identity          | [34] 9.2             | c11        | c7             | [34] 9.2             | n/a        | n/a            |
| 18I  | P-Preferred-Service           | [121] 4.2            | c32        | c31            | [121] 4.2            | n/a        | n/a            |
| 18J  | P-Private-Network-Indication  | [134]                | c36        | c36            | [134]                | c36        | c36            |
| 18K  | P-Profile-Key                 | [97] 5               | n/a        | n/a            | [97] 5               | n/a        | n/a            |
| 18L  | P-Served-User                 | [133] 6              | c41        | c41            | [133] 6              | c41        | c41            |
| 18M  | P-User-Database               | [82] 4               | n/a        | n/a            | [82] 4               | n/a        | n/a            |
| 18N  | P-Visited-Network-ID          | [52] 4.3             | x (note 1) | x              | [52] 4.3             | c14        | n/a            |
| 19   | Priority                      | [26] 20.26           | o          | o              | [26] 20.26           | o          | o              |
| 19A  | Privacy                       | [33] 4.2             | c12        | c12            | [33] 4.2             | c12        | c12            |
| 20   | Proxy-Authorization           | [26] 20.28           | c5         | c5             | [26] 20.28           | n/a        | n/a            |
| 21   | Proxy-Require                 | [26] 20.29           | o          | n/a            | [26] 20.29           | n/a        | n/a            |
| 21A  | Reason                        | [34A] 2              | c6         | c6             | [34A] 2              | c6         | c6             |
| 22   | Record-Route                  | [26] 20.30           | n/a        | c42            | [26] 20.30           | n/a        | c42            |
| 22A  | Referred-By                   | [59] 3               | c25        | c25            | [59] 3               | c26        | c26            |
| 23   | Reject-Contact                | [56B] 9.2            | c24        | c24            | [56B] 9.2            | c28        | c28            |
| 23A  | Reply-To                      | [26] 20.31           | o          | o              | [26] 20.31           | o          | o              |
| 23B  | Request-Disposition           | [56B] 9.1            | c24        | c24            | [56B] 9.1            | c28        | c28            |
| 24   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | m          | m              |
| 24A  | Resource-Priority             | [116] 3.1            | c30        | c30            | [116] 3.1            | c30        | c30            |
| 25   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | n/a        | n/a            |
| 25A  | Security-Client               | [48] 2.3.1           | c22        | c22            | [48] 2.3.1           | n/a        | n/a            |
| 25B  | Security-Verify               | [48] 2.3.1           | c23        | c23            | [48] 2.3.1           | n/a        | n/a            |
| 25C  | Session-ID                    | [162]                | o          | c43            | [162]                | o          | c43            |
| 26   | Subject                       | [26] 20.35           | o          | o              | [26] 20.36           | o          | o              |
| 27   | Supported                     | [26] 20.37           | c9         | m              | [26] 20.37           | m          | m              |
| 28   | Timestamp                     | [26] 20.38           | c10        | c10            | [26] 20.38           | m          | m              |
| 29   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 29A  | Trigger-Consent               | [125]<br>5.11.2      | c34        | c34            | [125]<br>5.11.2      | c35        | c35            |
| 30   | User-Agent                    | [26] 20.41           | o          | o              | [26] 20.41           | o          | o              |

| Item    | Header field  | Sending    |            |                | Receiving  |            |                |
|---------|---|------------|------------|----------------|------------|------------|----------------|
|         |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 31      | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:     | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.  |            |            |                |            |            |                |
| c2:     | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.  |            |            |                |            |            |                |
| c3:     | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.  |            |            |                |            |            |                |
| c4:     | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.  |            |            |                |            |            |                |
| c5:     | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.  |            |            |                |            |            |                |
| c6:     | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.  |            |            |                |            |            |                |
| c7:     | IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.   |            |            |                |            |            |                |
| c9:     | IF A.4/14 THEN m ELSE o - - support of reliable transport.  |            |            |                |            |            |                |
| c10:    | IF A.4/6 THEN o ELSE n/a - - timestamping of requests.  |            |            |                |            |            |                |
| c11:    | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |            |            |                |            |            |                |
| c12:    | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |            |            |                |            |            |                |
| c13:    | IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.  |            |            |                |            |            |                |
| c14:    | IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.   |            |            |                |            |            |                |
| c15:    | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.   |            |            |                |            |            |                |
| c16:    | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.  |            |            |                |            |            |                |
| c17:    | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.  |            |            |                |            |            |                |
| c18:    | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.   |            |            |                |            |            |                |
| c19:    | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |            |            |                |            |            |                |
| c20:    | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.   |            |            |                |            |            |                |
| c21:    | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |            |            |                |            |            |                |
| c22:    | IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 2).   |            |            |                |            |            |                |
| c23:    | IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |            |            |                |            |            |                |
| c24:    | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.   |            |            |                |            |            |                |
| c25:    | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |            |            |                |            |            |                |
| c26:    | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.  |            |            |                |            |            |                |
| c27:    | IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |            |            |                |            |            |                |
| c28:    | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |            |            |                |            |            |                |
| c29:    | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.  |            |            |                |            |            |                |
| c30:    | IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.   |            |            |                |            |            |                |
| c31:    | IF A.3/1 AND A.4/74 THEN o ELSE n/a - - UE and SIP extension for the identification of services.  |            |            |                |            |            |                |
| c32:    | IF A.4/74 THEN o ELSE n/a - - SIP extension for the identification of services.   |            |            |                |            |            |                |
| c33:    | IF A.4/74 THEN m ELSE n/a - - SIP extension for the identification of services.   |            |            |                |            |            |                |
| c34:    | IF A.4/75A THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP.  |            |            |                |            |            |                |
| c35:    | IF A.4/75B THEN m ELSE n/a - - a recipient within the framework for consent-based communications in SIP.  |            |            |                |            |            |                |
| c36:    | IF A.4/77 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).   |            |            |                |            |            |                |
| c39:    | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network. |            |            |                |            |            |                |
| c40:    | IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |            |            |                |            |            |                |
| c41:    | IF A.4/78 THEN m ELSE n/a - - the SIP P-Served-User private header.   |            |            |                |            |            |                |
| c42:    | IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.  |            |            |                |            |            |                |
| c43:    | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.  |            |            |                |            |            |                |
| c44:    | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.   |            |            |                |            |            |                |
| c45:    | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.  |            |            |                |            |            |                |
| c49:    | IF A.4/25 AND (A.3/7B OR A.3/8) THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and AS acting as originating UA, MRFC.  |            |            |                |            |            |                |
| c50:    | IF A.4/74 AND A.3/7B THEN o ELSE n/a - - SIP extension for the identification of services and AS acting as originating UA.  |            |            |                |            |            |                |
| NOTE 1: | The strength of this requirement in RFC 7315 [52] is SHOULD NOT, rather than MUST NOT.  |            |            |                |            |            |                |
| NOTE 2: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].   |            |            |                |            |            |                |

Prerequisite A.5/9A - - MESSAGE request

**Table A.62B: Supported message bodies within the MESSAGE request**

| Item | Header  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | permission document   | [125] 5.4 | c1         | c1             | [125] 5.4 | c2         | c2             |
| 2    | application/vnd.3gpp.sms  | [4D]      | c3         | c3             | [4D]      | c3         | c3             |
| 3    | message/cpim  | [151]     | c4         | c4             | [151]     | c4         | c4             |
| 4    | message/imdn+xml  | [157]     | c5         | c5             | [157]     | c5         | c5             |
| c1:  | IF A.4/75A THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP.                              |           |            |                |           |            |                |
| c2:  | IF A.4/75B THEN m ELSE n/a - - a recipient within the framework for consent-based communications in SIP.                          |           |            |                |           |            |                |
| c3:  | IF A.3A/61 OR A.3A/62 OR A.3A/63 THEN m ELSE o - - an SM-over-IP sender or an SM-over-IP receiver or an IP-SM-GW for SMS over IP. |           |            |                |           |            |                |
| c4:  | IF A.3A/71 AND A.4/85 THEN m ELSE n/a - - common presence and instant messaging (CPIM): message format.                           |           |            |                |           |            |                |
| c5:  | IF A.3A/71 AND A.4/86 THEN m ELSE n/a - - instant message disposition notification.   |           |            |                |           |            |                |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/1 - - Additional for 100 (Trying) response

**Table A.62BA: Supported header fields within the MESSAGE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID  | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length   | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq   | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date   | [26] 20.17 | c1         | c1             | [26] 20.17 | m          | m              |
| 5    | From   | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To   | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via  | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |            |            |                |            |            |                |



Prerequisite A.5/9B - - MESSAGE response for all remaining status-codes

**Table A.62C: Supported header fields within the MESSAGE response**

| Item | Header field   | Sending                          |            |                | Receiving                        |            |                |
|------|--|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |  | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow  | [26] 20.5                        | c12        | c12            | [26] 20.5                        | m          | m              |
| 1    | Call-ID  | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 2    | Call-Info  | [26] 20.9                        | o          | o              | [26] 20.9                        | o          | o              |
| 3    | Content-Disposition  | [26] 20.11                       | o (note 1) | o (note 1)     | [26] 20.11                       | m (note 1) | m (note 1)     |
| 4    | Content-Encoding   | [26] 20.12                       | o (note 1) | o (note 1)     | [26] 20.12                       | m (note 1) | m (note 1)     |
| 5    | Content-Language   | [26] 20.13                       | o (note 1) | o (note 1)     | [26] 20.13                       | m (note 1) | m (note 1)     |
| 6    | Content-Length   | [26] 20.14                       | m (note 1) | m (note 1)     | [26] 20.14                       | m (note 1) | m (note 1)     |
| 7    | Content-Type   | [26] 20.15                       | m (note 1) | m (note 1)     | [26] 20.15                       | m (note 1) | m (note 1)     |
| 8    | CSeq   | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 9    | Date   | [26] 20.17                       | c1         | c1             | [26] 20.17                       | m          | m              |
| 9A   | Expires  | [26] 20.19                       | o          | o              | [26] 20.19                       | o          | o              |
| 10   | From   | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 10A  | Geolocation-Error  | [89] 4.3                         | c14        | c14            | [89] 4.3                         | c14        | c14            |
| 10B  | History-Info   | [66] 4.1                         | c13        | c13            | [66] 4.1                         | c13        | c13            |
| 11   | MIME-Version   | [26] 20.24                       | o (note 1) | o (note 1)     | [26] 20.24                       | m (note 1) | m (note 1)     |
| 12   | Organization   | [26] 20.25                       | o          | o              | [26] 20.25                       | o          | o              |
| 12A  | P-Access-Network-Info  | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c6             | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c7             |
| 12B  | P-Asserted-Identity  | [34] 9.1                         | n/a        | c21            | [34] 9.1                         | c3         | c3             |
| 12C  | P-Charging-Function-Addresses  | [52] 4.5,<br>[52A] 4             | c10        | c11            | [52] 4.5,<br>[52A] 4             | c10        | c11            |
| 12D  | P-Charging-Vector  | [52] 4.6,<br>[52A] 4             | c8         | c9             | [52] 4.6,<br>[52A] 4             | c8         | c9             |
| 12F  | P-Preferred-Identity   | [34] 9.2                         | c3         | x              | [34] 9.2                         | n/a        | n/a            |
| 12G  | Privacy  | [33] 4.2                         | c4         | c4             | [33] 4.2                         | c4         | c4             |
| 12H  | Reply-To   | [26] 20.31                       | o          | o              | [26] 20.31                       | o          | o              |
| 12I  | Require  | [26] 20.32                       | m          | m              | [26] 20.32                       | m          | m              |
| 13   | Server   | [26] 20.35                       | o          | o              | [26] 20.35                       | o          | o              |
| 13A  | Session-ID   | [162]                            | o          | c17            | [162]                            | o          | c17            |
| 14   | Timestamp  | [26] 20.38                       | m          | m              | [26] 20.38                       | c2         | c2             |
| 15   | To   | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 16   | User-Agent   | [26] 20.41                       | o          | o              | [26] 20.41                       | o          | o              |
| 17   | Via  | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 18   | Warning  | [26] 20.43                       | o          | o              | [26] 20.43                       | o          | o              |
| c1:  | IF A.4/11 THEN o ELSE n/a -- insertion of date in requests and responses.  |                                  |            |                |                                  |            |                |
| c2:  | IF A.4/6 THEN m ELSE n/a -- timestamping of requests.  |                                  |            |                |                                  |            |                |
| c3:  | IF A.4/25 THEN o ELSE n/a -- private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |                                  |            |                |                                  |            |                |
| c4:  | IF A.4/26 THEN o ELSE n/a -- a privacy mechanism for the Session Initiation Protocol (SIP).  |                                  |            |                |                                  |            |                |
| c5:  | IF A.4/34 THEN o ELSE n/a -- the P-Access-Network-Info header extension.   |                                  |            |                |                                  |            |                |
| c6:  | IF A.4/34 AND A.3/1 THEN m ELSE n/a -- the P-Access-Network-Info header extension and UE.  |                                  |            |                |                                  |            |                |
| c7:  | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a -- the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.  |                                  |            |                |                                  |            |                |
| c8:  | IF A.4/36 THEN o ELSE n/a -- the P-Charging-Vector header extension.   |                                  |            |                |                                  |            |                |
| c9:  | IF A.4/36 THEN m ELSE n/a -- the P-Charging-Vector header extension.   |                                  |            |                |                                  |            |                |
| c10: | IF A.4/35 THEN o ELSE n/a -- the P-Charging-Function-Addresses header extension.   |                                  |            |                |                                  |            |                |
| c11: | IF A.4/35 THEN m ELSE n/a -- the P-Charging-Function-Addresses header extension.   |                                  |            |                |                                  |            |                |
| c12: | IF A.6/18 THEN m ELSE o -- 405 (Method Not Allowed).   |                                  |            |                |                                  |            |                |
| c13: | IF A.4/47 THEN m ELSE n/a -- an extension to the session initiation protocol for request history information.  |                                  |            |                |                                  |            |                |
| c14: | IF A.4/60 THEN m ELSE n/a -- SIP location conveyance.  |                                  |            |                |                                  |            |                |
| c17: | IF A.4/91 THEN m ELSE n/a -- the Session-ID header.  |                                  |            |                |                                  |            |                |
| c21: | IF A.4/25 AND (A.3/7B OR A.3/8 OR A.3A/83 OR A.3A/89) THEN o ELSE n/a -- private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and AS acting as originating UA, MRFC, SCC application server, ATCF (UA). |                                  |            |                |                                  |            |                |

NOTE 1: RFC 3428 [50] clause 7 states that all 2xx class responses to a MESSAGE request must not include any body, therefore for 2xx responses to the MESSAGE request the values on Sending side for "RFC status" and "Profile status" are "x", the values for Receiving side for "RFC status" and "Profile Status" are "n/a". RFC 3261 [26] subclause 7.4 states that all responses may contain bodies, therefore for all responses to the MESSAGE request other than 2xx responses, the values on Sending side for "RFC status" and "Profile status" are "o", the values for Receiving side for "RFC status" and "Profile Status" are "m".

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.62D: Supported header fields within the MESSAGE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Accept-Resource-Priority   | [116] 3.2  | c5         | c5             | [116] 3.2  | c5         | c5             |
| 1    | Allow-Events   | [28] 7.2.2 | c3         | c3             | [28] 7.2.2 | c4         | c4             |
| 2    | Authentication-Info  | [26] 20.6  | c1         | c1             | [26] 20.6  | c2         | c2             |
| 3    | Feature-Caps   | [190]      | c8         | c8             | [190]      | c7         | c7             |
| 6    | Supported  | [26] 20.37 | o          | o              | [26] 20.37 | m          | m              |
| c1:  | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c2:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c3:  | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.   |            |            |                |            |            |                |
| c4:  | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.   |            |            |                |            |            |                |
| c5:  | IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.  |            |            |                |            |            |                |
| c7:  | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.  |            |            |                |            |            |                |
| c8:  | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network. |            |            |                |            |            |                |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.62DA: Supported header fields within the MESSAGE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | o          | o              | [26] 20.18 | o          | o              |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/103 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.62E: Supported header fields within the MESSAGE response**

| Item  | Header field | Sending    |            |                | Receiving  |            |                |
|---|--------------|------------|------------|----------------|------------|------------|----------------|
|   |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2   | Contact      | [26] 20.10 | o (note)   | o              | [26] 20.10 | m          | m              |
| NOTE: The strength of this requirement is RECOMMENDED rather than OPTIONAL. |              |            |            |                |            |            |                |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.62F: Supported header fields within the MESSAGE response**

| Item | Header field       | Sending   |            |                | Receiving  |            |                |
|------|--------------------|---|------------|----------------|------------|------------|----------------|
|      |                    | Ref.  | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Proxy-Authenticate | [26] 20.27  | c1         | c1             | [26] 20.27 | c1         | c1             |
| 6    | WWW-Authenticate   | [26] 20.44  | m          | m              | [26] 20.44 | m          | m              |
| c1:  |                    | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |                |            |            |                |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.62G: Supported header fields within the MESSAGE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | o              |

**Table A.62H: Void**

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.62I: Supported header fields within the MESSAGE response**

| Item | Header field       | Sending   |            |                | Receiving  |            |                |
|------|--------------------|---|------------|----------------|------------|------------|----------------|
|      |                    | Ref.  | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Proxy-Authenticate | [26] 20.27  | c1         | c1             | [26] 20.27 | c1         | c1             |
| 6    | WWW-Authenticate   | [26] 20.44  | o          | o              | [26] 20.44 | o          | o              |
| c1:  |                    | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |                |            |            |                |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.62J: Supported header fields within the MESSAGE response**

| Item | Header field    | Sending  |            |                | Receiving |            |                |
|------|-----------------|--|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.   | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1  | o.1        | o.1            | [26] 20.1 | m          | m              |
| 2    | Accept-Encoding | [26] 20.2  | o.1        | o.1            | [26] 20.2 | m          | m              |
| 3    | Accept-Language | [26] 20.3  | o.1        | o.1            | [26] 20.3 | m          | m              |
| o.1  |                 | At least one of these capabilities is supported. |            |                |           |            |                |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.62JA: Supported header fields within the MESSAGE response**

| Item | Header field  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority  | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.62K: Supported header fields within the MESSAGE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | m          | m              |

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.62L: Supported header fields within the MESSAGE response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | x          | x              | [48] 2    | c1         | c1             |
| c1:  | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

**Table A.62M: Void**

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/29H - - Additional for 470 (Consent Needed) response

**Table A.62MA: Supported header fields within the MESSAGE response**

| Item | Header field       | Sending     |            |                | Receiving   |            |                |
|------|--------------------|-------------|------------|----------------|-------------|------------|----------------|
|      |                    | Ref.        | RFC status | Profile status | Ref.        | RFC status | Profile status |
| 1    | Permission-Missing | [125] 5.9.3 | m          | m              | [125] 5.9.3 | m          | m              |

Prerequisite A.5/9B - - MESSAGE response

**Table A.62N: Supported message bodies within the MESSAGE response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

### A.2.1.4.8 NOTIFY method

Prerequisite A.5/10 - - NOTIFY request

**Table A.63: Supported header fields within the NOTIFY request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | o          | o              | [26] 20.1            | m          | m              |
| 1A   | Accept-Contact                | [56B] 9.2            | c19        | c19            | [56B] 9.2            | c23        | c23            |
| 2    | Accept-Encoding               | [26] 20.2            | o          | o              | [26] 20.2            | m          | m              |
| 3    | Accept-Language               | [26] 20.3            | o          | o              | [26] 20.3            | m          | m              |
| 3A   | Allow                         | [26] 20.5            | o          | o              | [26] 20.5            | m          | m              |
| 4    | Allow-Events                  | [28] 7.2.2           | c1         | c1             | [28] 7.2.2           | c2         | c2             |
| 5    | Authorization                 | [26] 20.7            | c3         | c3             | [26] 20.7            | c3         | c3             |
| 6    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 6A   | Call-Info                     | [26] 20.9            | o          | o              | [26] 20.9            | c25        | c25            |
| 6B   | Contact                       | [26] 20.10           | m          | m              | [26] 20.10           | m          | m              |
| 7    | Content-Disposition           | [26] 20.11           | o          | o              | [26] 20.11           | m          | m              |
| 8    | Content-Encoding              | [26] 20.12           | o          | o              | [26] 20.12           | m          | m              |
| 9    | Content-Language              | [26] 20.13           | o          | o              | [26] 20.13           | m          | m              |
| 10   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 11   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | m          | m              |
| 12   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 13   | Date                          | [26] 20.17           | c4         | c4             | [26] 20.17           | m          | m              |
| 14   | Event                         | [28] 7.2.1           | m          | m              | [28] 7.2.1           | m          | m              |
| 14A  | Feature-Caps                  | [190]                | c35        | c35            | [190]                | c34        | c34            |
| 15   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 15A  | Geolocation                   | [89] 4.1             | c24        | c24            | [89] 4.1             | c24        | c24            |
| 15B  | Geolocation-Routing           | [89] 4.2             | c24        | c24            | [89] 4.2             | c24        | c24            |
| 15C  | History-Info                  | [66] 4.1             | c22        | c22            | [66] 4.1             | c22        | c22            |
| 15D  | Max-Breadth                   | [117] 5.8            | n/a        | c26            | [117] 5.8            | c27        | c27            |
| 16   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | n/a        | c32            |
| 17   | MIME-Version                  | [26] 20.24           | o          | o              | [26] 20.24           | m          | m              |
| 17A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c10        | c11            | [52] 4.4,<br>[234] 2 | c10        | c12            |
| 17B  | P-Asserted-Identity           | [34] 9.1             | n/a        | c40            | [34] 9.1             | c6         | c6             |
| 17C  | P-Charging-Function-Addresses | [52] 4.5             | c14        | c15            | [52] 4.5             | c14        | c15            |
| 17D  | P-Charging-Vector             | [52] 4.6             | c13        | n/a            | [52] 4.6             | c13        | n/a            |
| 17F  | P-Preferred-Identity          | [34] 9.2             | c6         | x              | [34] 9.2             | n/a        | n/a            |
| 17G  | Privacy                       | [33] 4.2             | c7         | n/a            | [33] 4.2             | c7         | c7             |
| 18   | Proxy-Authorization           | [26] 20.28           | c5         | c5             | [26] 20.28           | n/a        | n/a            |
| 19   | Proxy-Require                 | [26] 20.29           | o          | n/a            | [26] 20.29           | n/a        | n/a            |
| 19A  | Reason                        | [34A] 2              | c18        | c18            | [34A] 2              | c18        | c18            |
| 20   | Record-Route                  | [26] 20.30           | n/a        | c32            | [26] 20.30           | c9         | c9             |
| 20A  | Referred-By                   | [59] 3               | c20        | c20            | [59] 3               | c21        | c21            |
| 20B  | Reject-Contact                | [56B] 9.2            | c19        | c19            | [56B] 9.2            | c23        | c23            |
| 20C  | Request-Disposition           | [56B] 9.1            | c19        | c19            | [56B] 9.1            | c23        | c23            |
| 21   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | m          | m              |
| 22A  | Resource-Priority             | [116] 3.1            | c29        | c29            | [116] 3.1            | c29        | c29            |
| 22B  | Security-Client               | [48] 2.3.1           | c16        | c16            | [48] 2.3.1           | n/a        | n/a            |
| 22C  | Security-Verify               | [48] 2.3.1           | c17        | c17            | [48] 2.3.1           | n/a        | n/a            |
| 22D  | Session-ID                    | [162]                | o          | c33            | [162]                | o          | c33            |
| 22   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | n/a        | c32            |
| 23   | Subscription-State            | [28] 8.2.3           | m          | m              | [28] 8.2.3           | m          | m              |
| 24   | Supported                     | [26] 20.37           | o          | o              | [26] 20.37           | m          | m              |
| 25   | Timestamp                     | [26] 20.38           | c8         | c8             | [26] 20.38           | m          | m              |
| 26   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 27   | User-Agent                    | [26] 20.41           | o          | o              | [26] 20.41           | o          | o              |
| 28   | Via                           | [26] 20.42           | m          | m              | [26] 20.42           | m          | m              |
| 29   | Warning                       | [26] 20.43           | o          | o              | [26] 20.43           | o          | o              |

|       |   |
|-------|---|
| c1:   | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension.  |
| c2:   | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.  |
| c3:   | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.  |
| c4:   | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.  |
| c5:   | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.  |
| c6:   | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c7:   | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c8:   | IF A.4/6 THEN o ELSE n/a - - timestamping of requests.  |
| c9:   | IF A.4/15 OR A.4/20 THEN m ELSE n/a - - the REFER method extension or SIP specific event notification extension.  |
| c10:  | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.   |
| c11:  | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.  |
| c12:  | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.  |
| c13:  | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.   |
| c14:  | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c15:  | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c16:  | IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note).   |
| c17:  | IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |
| c18:  | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c19:  | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.   |
| c20:  | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c21:  | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.  |
| c22:  | IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c23:  | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c24:  | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.  |
| c25:  | IF A.4/63 THEN m ELSE o - - subscriptions to request-contained resource lists in the session initiation protocol.   |
| c26:  | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network. |
| c27:  | IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |
| c29:  | IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.   |
| c32:: | IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.  |
| c33:  | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.  |
| c34:  | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.   |
| c35:  | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.  |
| c40:  | IF A.4/25 AND (A.3/7B OR A.3/8) THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and AS acting as originating UA, MRFC.  |
| NOTE: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].   |

Prerequisite A.5/10 - - NOTIFY request

**Table A.64: Supported message bodies within the NOTIFY request**

| Item  | Header  | Sending |            |                | Receiving |            |                |
|-------|---|---------|------------|----------------|-----------|------------|----------------|
|       |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1     | sipfrag   | [37] 2  | c1         | c1             | [37]      | c1         | c1             |
| 2     | event package (see NOTE)  | [28]    | m          | m              | [28]      | m          | m              |
| c1:   | IF A.4/15 THEN m ELSE o - - the REFER method extension  |         |            |                |           |            |                |
| NOTE: | The appropriate body specified for the supported event package (see table A.4A) is supported. |         |            |                |           |            |                |



Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/1 - - Additional for 100 (Trying) response

**Table A.64A: Supported header fields within the NOTIFY response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID  | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length   | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq   | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date   | [26] 20.17 | c1         | c1             | [26] 20.17 | m          | m              |
| 5    | From   | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To   | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via  | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |            |            |                |            |            |                |

Prerequisite A.5/11 - - NOTIFY response for all remaining status-codes

**Table A.65: Supported header fields within the NOTIFY response**

| Item  | Header field   | Sending                          |            |                | Receiving                        |            |                |
|-------|--|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|       |  | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A    | Allow  | [26] 20.5                        | o          | o              | [26] 20.5                        | m          | m              |
| 1     | Call-ID  | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 2     | Content-Disposition  | [26] 20.11                       | o          | o              | [26] 20.11                       | m          | m              |
| 3     | Content-Encoding   | [26] 20.12                       | o          | o              | [26] 20.12                       | m          | m              |
| 4     | Content-Language   | [26] 20.13                       | o          | o              | [26] 20.13                       | m          | m              |
| 5     | Content-Length   | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6     | Content-Type   | [26] 20.15                       | m          | m              | [26] 20.15                       | m          | m              |
| 7     | CSeq   | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8     | Date   | [26] 20.17                       | c1         | c1             | [26] 20.17                       | m          | m              |
| 9     | From   | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A    | Geolocation-Error  | [89] 4.3                         | c12        | c12            | [89] 4.3                         | c12        | c12            |
| 10    | MIME-Version   | [26] 20.24                       | o          | o              | [26] 20.24                       | m          | m              |
| 10A   | P-Access-Network-Info  | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c6             | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c7             |
| 10B   | P-Asserted-Identity  | [34] 9.1                         | n/a        | c20            | [34] 9.1                         | c3         | c3             |
| 10C   | P-Charging-Function-Addresses  | [52] 4.5,<br>[52A] 4             | c9         | c10            | [52] 4.5,<br>[52A] 4             | c9         | c10            |
| 10D   | P-Charging-Vector  | [52] 4.6,<br>[52A] 4             | c8         | n/a            | [52] 4.6,<br>[52A] 4             | c8         | n/a            |
| 10F   | P-Preferred-Identity   | [34] 9.2                         | c3         | x              | [34] 9.2                         | n/a        | n/a            |
| 10G   | Privacy  | [33] 4.2                         | c4         | n/a            | [33] 4.2                         | c4         | c4             |
| 10H   | Require  | [26] 20.32                       | m          | m              | [26] 20.32                       | m          | m              |
| 10I   | Server   | [26] 20.35                       | o          | o              | [26] 20.35                       | o          | o              |
| 10J   | Session-ID   | [162]                            | o          | c15            | [162]                            | o          | c15            |
| 11    | Timestamp  | [26] 20.38                       | m          | m              | [26] 20.38                       | c2         | c2             |
| 12    | To   | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 12A   | User-Agent   | [26] 20.41                       | o          | o              | [26] 20.41                       | o          | o              |
| 13    | Via  | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 14    | Warning  | [26] 20.43                       | o (note)   | o              | [26] 20.43                       | o          | o              |
| c1:   | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c2:   | IF A.4/6 THEN m ELSE n/a - - timestamping of requests.   |                                  |            |                |                                  |            |                |
| c3:   | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.   |                                  |            |                |                                  |            |                |
| c4:   | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |                                  |            |                |                                  |            |                |
| c5:   | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.  |                                  |            |                |                                  |            |                |
| c6:   | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.   |                                  |            |                |                                  |            |                |
| c7:   | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.                         |                                  |            |                |                                  |            |                |
| c8:   | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c9:   | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c10:  | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c11:  | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).  |                                  |            |                |                                  |            |                |
| c12:  | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.   |                                  |            |                |                                  |            |                |
| c15:  | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |
| c20:  | IF A.4/25 AND (A.3/7B OR A.3/8) THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and AS acting as originating UA, MRFC. |                                  |            |                |                                  |            |                |
| NOTE: | RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.  |                                  |            |                |                                  |            |                |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.66: Supported header fields within the NOTIFY response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Accept-Resource-Priority  | [116] 3.2  | c6         | c6             | [116] 3.2  | c6         | c6             |
| 0B   | Allow-Events  | [28] 7.2.2 | c4         | c4             | [28] 7.2.2 | c5         | c5             |
| 1    | Authentication-Info   | [26] 20.6  | c1         | c1             | [26] 20.6  | c2         | c2             |
| 1A   | Contact   | [26] 20.10 | o          | o              | [26] 20.10 | m          | m              |
| 1B   | Feature-Caps  | [190]      | c8         | c8             | [190]      | c8         | c8             |
| 2    | Record-Route  | [26] 20.30 | c3         | c3             | [26] 20.30 | c3         | c3             |
| 5    | Supported   | [26] 20.37 | m          | m              | [26] 20.37 | m          | m              |
| c1:  | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.  |            |            |                |            |            |                |
| c2:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.  |            |            |                |            |            |                |
| c3:  | IF A.4/15 OR A.4/20 THEN m ELSE n/a - - the REFER method extension or SIP specific event notification extension.                                |            |            |                |            |            |                |
| c4:  | IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension.  |            |            |                |            |            |                |
| c5:  | IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.  |            |            |                |            |            |                |
| c6:  | IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol. |            |            |                |            |            |                |
| c8:  | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.   |            |            |                |            |            |                |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.66A: Supported header fields within the NOTIFY response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | o          | o              | [26] 20.18 | o          | o              |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/103 - - Additional for 3xx response

**Table A.67: Supported header fields within the NOTIFY response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Contact      | [26] 20.10 | m          | m              | [26] 20.10 | m          | m              |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.68: Supported header fields within the NOTIFY response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate  | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 8    | WWW-Authenticate  | [26] 20.44 | m          | m              | [26] 20.44 | m          | m              |
| c1:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.69: Supported header fields within the NOTIFY response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | o              |

**Table A.70: Void**

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.71: Supported header fields within the NOTIFY response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate  | [26] 20.27 | c3         | c3             | [26] 20.27 | c3         | c3             |
| 6    | WWW-Authenticate  | [26] 20.44 | o          | o              | [26] 20.44 | o          | o              |
| c3:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.72: Supported header fields within the NOTIFY response**

| Item | Header field                                     | Sending   |            |                | Receiving |            |                |
|------|--|-----------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept   | [26] 20.1 | o.1        | o.1            | [26] 20.1 | m          | m              |
| 2    | Accept-Encoding                                  | [26] 20.2 | o.1        | o.1            | [26] 20.2 | m          | m              |
| 3    | Accept-Language                                  | [26] 20.3 | o.1        | o.1            | [26] 20.3 | m          | m              |
| o.1  | At least one of these capabilities is supported. |           |            |                |           |            |                |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.72A: Supported header fields within the NOTIFY response**

| Item | Header field  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority  | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/27 - - Addition for 420 (Bad Extension) response

**Table A.73: Supported header fields within the NOTIFY response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | m          | m              |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.73A: Supported header fields within the NOTIFY response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | x          | x              | [48] 2    | c1         | c1             |
| c1:  | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

**Table A.74: Void**

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/35 - - Additional for 485 (Ambiguous) response

**Table A.74A: Supported header fields within the NOTIFY response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Contact      | [26] 20.10 | o          | o              | [26] 20.10 | m          | m              |

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/39 - - Additional for 489 (Bad Event) response

**Table A.75: Supported header fields within the NOTIFY response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Allow-Events | [28] 7.2.2 | m          | m              | [28] 7.2.2 | m          | m              |

Prerequisite A.5/11 - - NOTIFY response

**Table A.76: Supported message bodies within the NOTIFY response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

#### A.2.1.4.9 OPTIONS method

Prerequisite A.5/12 - - OPTIONS request

**Table A.77: Supported header fields within the OPTIONS request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | m          | m              | [26] 20.1            | m          | m              |
| 1A   | Accept-Contact                | [56B] 9.2            | c21        | c21            | [56B] 9.2            | c26        | c26            |
| 2    | Accept-Encoding               | [26] 20.2            | m          | m              | [26] 20.2            | m          | m              |
| 3    | Accept-Language               | [26] 20.3            | m          | m              | [26] 20.3            | m          | m              |
| 3A   | Allow                         | [26] 20.5            | o          | o              | [26] 20.5            | m          | m              |
| 4    | Allow-Events                  | [28] 7.2.2           | c24        | c24            | [28] 7.2.2           | c1         | c1             |
| 5    | Authorization                 | [26] 20.7            | c2         | c2             | [26] 20.7            | c2         | c2             |
| 6    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 7    | Call-Info                     | [26] 20.9            | o          | o              | [26] 20.9            | o          | o              |
| 8    | Contact                       | [26] 20.10           | o          | o              | [26] 20.10           | o          | o              |
| 9    | Content-Disposition           | [26] 20.11           | o          | o              | [26] 20.11           | m          | m              |
| 10   | Content-Encoding              | [26] 20.12           | o          | o              | [26] 20.12           | m          | m              |
| 11   | Content-Language              | [26] 20.13           | o          | o              | [26] 20.13           | m          | m              |
| 12   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 13   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | m          | m              |
| 14   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 15   | Date                          | [26] 20.17           | c3         | c3             | [26] 20.17           | m          | m              |
| 15A  | Feature-Caps                  | [190]                | c42        | c42            | [190]                | c41        | c41            |
| 16   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 16A  | Geolocation                   | [89] 4.1             | c27        | c27            | [89] 4.1             | c27        | c27            |
| 16B  | Geolocation-Routing           | [89] 4.2             | c27        | c27            | [89] 4.2             | c27        | c27            |
| 16C  | History-Info                  | [66] 4.1             | c25        | c25            | [66] 4.1             | c25        | c25            |
| 16D  | Max-Breadth                   | [117] 5.8            | n/a        | c31            | [117] 5.8            | c32        | c32            |
| 17   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | n/a        | c39            |
| 18   | MIME-Version                  | [26] 20.24           | o          | o              | [26] 20.24           | m          | m              |
| 19   | Organization                  | [26] 20.25           | o          | o              | [26] 20.25           | o          | o              |
| 19A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c11        | c12            | [52] 4.4,<br>[234] 2 | c11        | c13            |
| 19B  | P-Asserted-Identity           | [34] 9.1             | n/a        | c46            | [34] 9.1             | c6         | c6             |
| 19C  | P-Asserted-Service            | [121] 4.1            | n/a        | c47            | [121] 4.1            | c30        | c30            |
| 19D  | P-Called-Party-ID             | [52] 4.2             | x          | x              | [52] 4.2             | c9         | c9             |
| 19E  | P-Charging-Function-Addresses | [52] 4.5             | c16        | c17            | [52] 4.5             | c16        | c17            |
| 19F  | P-Charging-Vector             | [52] 4.6             | c14        | c15            | [52] 4.6             | c14        | c15            |
| 19H  | P-Preferred-Identity          | [34] 9.2             | c6         | c4             | [34] 9.2             | n/a        | n/a            |
| 19I  | P-Preferred-Service           | [121] 4.2            | c29        | c28            | [121] 4.2            | n/a        | n/a            |
| 19J  | P-Private-Network-Indication  | [134]                | c34        | c34            | [134]                | c34        | c34            |
| 19K  | P-Profile-Key                 | [97] 5               | n/a        | n/a            | [97] 5               | n/a        | n/a            |
| 19L  | P-Served-User                 | [133] 6              | c38        | c38            | [133] 6              | c38        | c38            |
| 19M  | P-User-Database               | [82] 4               | n/a        | n/a            | [82] 4               | n/a        | n/a            |
| 19N  | P-Visited-Network-ID          | [52] 4.3             | x (note 2) | x              | [52] 4.3             | c10        | n/a            |
| 19O  | Privacy                       | [33] 4.2             | c8         | c8             | [33] 4.2             | c8         | c8             |
| 20   | Proxy-Authorization           | [26] 20.28           | c5         | c5             | [26] 20.28           | n/a        | n/a            |
| 21   | Proxy-Require                 | [26] 20.29           | o          | o (note 1)     | [26] 20.29           | n/a        | n/a            |
| 21A  | Reason                        | [34A] 2              | c20        | c20            | [34A] 2              | c20        | c20            |
| 22   | Record-Route                  | [26] 20.30           | n/a        | c39            | [26] 20.30           | n/a        | c39            |
| 22A  | Recv-Info                     | [25] 5.2.3           | c37        | c37            | [25] 5.2.3           | c37        | c37            |
| 22B  | Referred-By                   | [59] 3               | c22        | c22            | [59] 3               | c23        | c23            |
| 22C  | Reject-Contact                | [56B] 9.2            | c21        | c21            | [56B] 9.2            | c26        | c26            |
| 22D  | Request-Disposition           | [56B] 9.1            | c21        | c21            | [56B] 9.1            | c26        | c26            |
| 23   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | m          | m              |
| 23A  | Resource-Priority             | [116] 3.1            | c33        | c33            | [116] 3.1            | c33        | c33            |
| 24   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | n/a        | n/a            |
| 24A  | Security-Client               | [48] 2.3.1           | c18        | c18            | [48] 2.3.1           | n/a        | n/a            |
| 24B  | Security-Verify               | [48] 2.3.1           | c19        | c19            | [48] 2.3.1           | n/a        | n/a            |
| 24C  | Session-ID                    | [162]                | o          | c40            | [162]                | o          | c40            |
| 25   | Supported                     | [26] 20.37           | c6         | c6             | [26] 20.37           | m          | m              |
| 26   | Timestamp                     | [26] 20.38           | c7         | c7             | [26] 20.38           | m          | m              |
| 27   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 28   | User-Agent                    | [26] 20.41           | o          | o              | [26] 20.41           | o          | o              |
| 29   | Via                           | [26] 20.42           | m          | m              | [26] 20.42           | m          | m              |



|         |  |
|---------|--|
| c1:     | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.   |
| c2:     | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.   |
| c3:     | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.   |
| c4:     | IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c5:     | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.   |
| c6:     | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.   |
| c7:     | IF A.4/6 THEN o ELSE n/a - - timestamping of requests.   |
| c8:     | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |
| c9:     | IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.   |
| c10:    | IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.  |
| c11:    | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.  |
| c12:    | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.   |
| c13:    | IF A.4/34 AND (A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA, AS acting as third-party call controller or EATF.   |
| c14:    | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.  |
| c15:    | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.  |
| c16:    | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.  |
| c17:    | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.  |
| c18:    | IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 3).  |
| c19:    | IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.   |
| c20:    | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.   |
| c21:    | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.  |
| c22:    | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.   |
| c23:    | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.   |
| c24:    | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.   |
| c25:    | IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.   |
| c26:    | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.  |
| c27:    | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.   |
| c28:    | IF (A.3/1 OR A.3A/81) AND A.4/74 THEN o ELSE n/a - - UE, MSC Server enhanced for ICS and SIP extension for the identification of services.   |
| c29:    | IF A.4/74 THEN o ELSE n/a - - SIP extension for the identification of services.  |
| c30:    | IF A.4/74 THEN m ELSE n/a - - SIP extension for the identification of services.  |
| c31:    | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13) THEN m ELSE IF A.3/1 AND NOT A.3C/1 - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network. |
| c32:    | IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.  |
| c33:    | IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.  |
| c34:    | IF A.4/77 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).  |
| c37:    | IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.   |
| c38:    | IF A.4/78 THEN m ELSE n/a - - the SIP P-Served-User private header.  |
| c39:    | IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.   |
| c40:    | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.   |
| c41:    | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.  |
| c42:    | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.   |
| c46:    | IF A.4/25 AND (A.3/7B OR A.3/8) THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and AS acting as originating UA, MRFC.   |
| c47:    | IF A.4/74 AND A.3/7B THEN o ELSE n/a - - SIP extension for the identification of services and AS acting as originating UA.   |
| NOTE 1: | No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.  |
| NOTE 2: | The strength of this requirement in RFC 7315 [52] is SHOULD NOT, rather than MUST NOT.   |
| NOTE 3: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].  |

Prerequisite A.5/12 - - OPTIONS request

**Table A.78: Supported message bodies within the OPTIONS request**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

**Table A.79: Void**

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/1 - - Additional for 100 (Trying) response

**Table A.79A: Supported header fields within the OPTIONS response**

| Item | Header field   | Sending  |            |                | Receiving  |            |                |
|------|----------------|--|------------|----------------|------------|------------|----------------|
|      |                | Ref.   | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID        | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length | [26] 20.14   | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq           | [26] 20.16   | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date           | [26] 20.17   | c1         | c1             | [26] 20.17 | m          | m              |
| 5    | From           | [26] 20.20   | m          | m              | [26] 20.20 | m          | m              |
| 6    | To             | [26] 20.39   | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via            | [26] 20.42   | m          | m              | [26] 20.42 | m          | m              |
| c1:  |                | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |            |                |            |            |                |

Prerequisite A.5/13 - - OPTIONS response for all remaining status-codes

**Table A.80: Supported header fields within the OPTIONS response**

| Item  | Header field   | Sending                          |            |                | Receiving                        |            |                |
|-------|--|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|       |  | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A    | Allow  | [26] 20.5                        | c12        | c12            | [26] 20.5                        | m          | m              |
| 1     | Call-ID  | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 1A    | Call-Info  | [26] 20.9                        | o          | o              | [26] 20.9                        | o          | o              |
| 2     | Content-Disposition  | [26] 20.11                       | o          | o              | [26] 20.11                       | m          | m              |
| 3     | Content-Encoding   | [26] 20.12                       | o          | o              | [26] 20.12                       | m          | m              |
| 4     | Content-Language   | [26] 20.13                       | o          | o              | [26] 20.13                       | m          | m              |
| 5     | Content-Length   | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6     | Content-Type   | [26] 20.15                       | m          | m              | [26] 20.15                       | m          | m              |
| 7     | CSeq   | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8     | Date   | [26] 20.17                       | c1         | c1             | [26] 20.17                       | m          | m              |
| 9     | From   | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A    | Geolocation-Error  | [89] 4.3                         | c14        | c14            | [89] 4.3                         | c14        | c14            |
| 9B    | History-Info   | [66] 4.1                         | c13        | c13            | [66] 4.1                         | c13        | c13            |
| 10    | MIME-Version   | [26] 20.24                       | o          | o              | [26] 20.24                       | m          | m              |
| 11    | Organization   | [26] 20.25                       | o          | o              | [26] 20.25                       | o          | o              |
| 11A   | P-Access-Network-Info  | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c6             | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c7             |
| 11B   | P-Asserted-Identity  | [34] 9.1                         | n/a        | c22            | [34] 9.1                         | c3         | c3             |
| 11C   | P-Charging-Function-Addresses  | [52] 4.5,<br>[52A] 4             | c10        | c11            | [52] 4.5,<br>[52A] 4             | c10        | c11            |
| 11D   | P-Charging-Vector  | [52] 4.6,<br>[52A] 4             | c8         | c9             | [52] 4.6,<br>[52A] 4             | c8         | c9             |
| 11F   | P-Preferred-Identity   | [34] 9.2                         | c3         | x              | [34] 9.2                         | n/a        | n/a            |
| 11G   | Privacy  | [33] 4.2                         | c4         | c4             | [33] 4.2                         | c4         | c4             |
| 11H   | Recv-Info  | [25] 5.2.3                       | c17        | c17            | [25] 5.2.3                       | c17        | c17            |
| 11I   | Require  | [26] 20.32                       | m          | m              | [26] 20.32                       | m          | m              |
| 11J   | Server   | [26] 20.35                       | o          | o              | [26] 20.35                       | o          | o              |
| 11K   | Session-ID   | [162]                            | o          | c18            | [162]                            | o          | c18            |
| 12    | Timestamp  | [26] 20.38                       | m          | m              | [26] 20.38                       | c2         | c2             |
| 13    | To   | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 13A   | User-Agent   | [26] 20.41                       | o          | o              | [26] 20.41                       | o          | o              |
| 14    | Via  | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 15    | Warning  | [26] 20.43                       | o (note)   | o              | [26] 20.43                       | o          | o              |
| c1:   | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c2:   | IF A.4/6 THEN m ELSE n/a - - timestamping of requests.   |                                  |            |                |                                  |            |                |
| c3:   | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.   |                                  |            |                |                                  |            |                |
| c4:   | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |                                  |            |                |                                  |            |                |
| c5:   | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.  |                                  |            |                |                                  |            |                |
| c6:   | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.   |                                  |            |                |                                  |            |                |
| c7:   | IF A.4/34 AND (A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA, AS acting as third-party call controller, or EATF.        |                                  |            |                |                                  |            |                |
| c8:   | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c9:   | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c10:  | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c11:  | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c12:  | IF A.6/6 OR A.6/18 THEN m ELSE o - - 200 (OK), 405 (Method Not Allowed).   |                                  |            |                |                                  |            |                |
| c13:  | IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.   |                                  |            |                |                                  |            |                |
| c14:  | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.   |                                  |            |                |                                  |            |                |
| c17:  | IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.   |                                  |            |                |                                  |            |                |
| c18:  | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |
| c22:  | IF A.4/25 AND (A.3/7B OR A.3/8) THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and AS acting as originating UA, MRFC. |                                  |            |                |                                  |            |                |
| NOTE: | RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.  |                                  |            |                |                                  |            |                |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.81: Supported header fields within the OPTIONS response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Accept   | [26] 20.1  | m          | m              | [26] 20.1  | m          | m              |
| 1A   | Accept-Encoding  | [26] 20.2  | m          | m              | [26] 20.2  | m          | m              |
| 1B   | Accept-Language  | [26] 20.3  | m          | m              | [26] 20.3  | m          | m              |
| 1C   | Accept-Resource-Priority   | [116] 3.2  | c14        | c14            | [116] 3.2  | c14        | c14            |
| 2    | Allow-Events   | [28] 7.2.2 | c3         | c3             | [28] 7.2.2 | c4         | c4             |
| 3    | Authentication-Info  | [26] 20.6  | c1         | c1             | [26] 20.6  | c2         | c2             |
| 5    | Contact  | [26] 20.10 | o          | o              | [26] 20.10 | o          | o              |
| 6    | Feature-Caps   | [190]      | c16        | c16            | [190]      | c15        | c15            |
| 7    | Recv-Info  | [25] 5.2.3 | c6         | c6             | [25] 5.2.3 | c6         | c6             |
| 12   | Supported  | [26] 20.37 | m          | m              | [26] 20.37 | m          | m              |
| c1:  | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c2:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c3:  | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.   |            |            |                |            |            |                |
| c4:  | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.   |            |            |                |            |            |                |
| c6:  | IF A.4/13 THEN m ELSE n/a - - SIP INFO method and package framework.   |            |            |                |            |            |                |
| c14: | IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.  |            |            |                |            |            |                |
| c15: | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.  |            |            |                |            |            |                |
| c16: | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network. |            |            |                |            |            |                |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.81A: Supported header fields within the OPTIONS response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | o          | o              | [26] 20.18 | o          | o              |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.82: Supported header fields within the OPTIONS response**

| Item  | Header field  | Sending    |            |                | Receiving  |            |                |
|-------|---|------------|------------|----------------|------------|------------|----------------|
|       |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3     | Contact   | [26] 20.10 | o (note)   | o              | [26] 20.10 | m          | m              |
| NOTE: | RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL. |            |            |                |            |            |                |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.83: Supported header fields within the OPTIONS response**

| Item | Header field       | Sending   |            |                | Receiving  |            |                |
|------|--------------------|---|------------|----------------|------------|------------|----------------|
|      |                    | Ref.  | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Proxy-Authenticate | [26] 20.27  | c1         | c1             | [26] 20.27 | c1         | c1             |
| 10   | WWW-Authenticate   | [26] 20.44  | o          | o              | [26] 20.44 | o          | o              |
| c1:  |                    | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |                |            |            |                |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480 (Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response.

**Table A.84: Supported header fields within the OPTIONS response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | o              |

**Table A.85: Void**

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.86: Supported header fields within the OPTIONS response**

| Item | Header field       | Sending   |            |                | Receiving  |            |                |
|------|--------------------|---|------------|----------------|------------|------------|----------------|
|      |                    | Ref.  | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Proxy-Authenticate | [26] 20.27  | c1         | c1             | [26] 20.27 | c1         | c1             |
| 8    | WWW-Authenticate   | [26] 20.44  | o          | o              | [26] 20.44 | o          | o              |
| c1:  |                    | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |                |            |            |                |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.87: Supported header fields within the OPTIONS response**

| Item | Header field    | Sending  |            |                | Receiving |            |                |
|------|-----------------|--|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.   | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1  | o.1        | o.1            | [26] 20.1 | m          | m              |
| 2    | Accept-Encoding | [26] 20.2  | o.1        | o.1            | [26] 20.2 | m          | m              |
| 3    | Accept-Language | [26] 20.3  | o.1        | o.1            | [26] 20.3 | m          | m              |
| o.1  |                 | At least one of these capabilities is supported. |            |                |           |            |                |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.87A: Supported header fields within the OPTIONS response**

| Item  | Header field             | Sending   |            |                | Receiving |            |                |
|---|--------------------------|-----------|------------|----------------|-----------|------------|----------------|
|   |                          | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1   | Accept-Resource-Priority | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1: IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol. |                          |           |            |                |           |            |                |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.88: Supported header fields within the OPTIONS response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 7    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | m          | m              |

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/28 OR A.6/41A - - Additional 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.88A: Supported header fields within the OPTIONS response**

| Item  | Header field    | Sending |            |                | Receiving |            |                |
|---|-----------------|---------|------------|----------------|-----------|------------|----------------|
|   |                 | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3   | Security-Server | [48] 2  | x          | x              | [48] 2    | c1         | c1             |
| c1: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |                 |         |            |                |           |            |                |

**Table A.89: Void**

Prerequisite A.5/13 - - OPTIONS response

**Table A.90: Supported message bodies within the OPTIONS response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

## A.2.1.4.10 PRACK method

Prerequisite A.5/14 - - PRACK request

**Table A.91: Supported header fields within the PRACK request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | o          | o              | [26] 20.1            | m          | m              |
| 1A   | Accept-Contact                | [56B] 9.2            | c15        | c15            | [56B] 9.2            | c18        | c18            |
| 2    | Accept-Encoding               | [26] 20.2            | o          | o              | [26] 20.2            | m          | m              |
| 3    | Accept-Language               | [26] 20.3            | o          | o              | [26] 20.3            | m          | m              |
| 3A   | Allow                         | [26] 20.5            | o          | o              | [26] 20.5            | m          | m              |
| 4    | Allow-Events                  | [28] 7.2.2           | c1         | c1             | [28] 7.2.2           | c2         | c2             |
| 5    | Authorization                 | [26] 20.7            | c3         | c3             | [26] 20.7            | c3         | c3             |
| 6    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 7    | Content-Disposition           | [26] 20.11           | o          | o              | [26] 20.11           | m          | m              |
| 8    | Content-Encoding              | [26] 20.12           | o          | o              | [26] 20.12           | m          | m              |
| 9    | Content-Language              | [26] 20.13           | o          | o              | [26] 20.13           | m          | m              |
| 10   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 11   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | m          | m              |
| 12   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 13   | Date                          | [26] 20.17           | c4         | c4             | [26] 20.17           | m          | m              |
| 14   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 14A  | Max-Breadth                   | [117] 5.8            | n/a        | c21            | [117] 5.8            | c22        | c22            |
| 15   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | n/a        | c34            |
| 16   | MIME-Version                  | [26] 20.24           | o          | o              | [26] 20.24           | m          | m              |
| 16A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c9         | c10            | [52] 4.4,<br>[234] 2 | c9         | c11            |
| 16B  | P-Charging-Function-Addresses | [52] 4.5             | c13        | c14            | [52] 4.5             | c13        | c14            |
| 16C  | P-Charging-Vector             | [52] 4.6             | c12        | n/a            | [52] 4.6             | c12        | n/a            |
| 16E  | Privacy                       | [33] 4.2             | c6         | n/a            | [33] 4.2             | c6         | n/a            |
| 17   | Proxy-Authorization           | [26] 20.28           | c5         | c5             | [26] 20.28           | n/a        | n/a            |
| 18   | Proxy-Require                 | [26] 20.29           | o          | n/a            | [26] 20.29           | n/a        | n/a            |
| 19   | RAck                          | [27] 7.2             | m          | m              | [27] 7.2             | m          | m              |
| 19A  | Reason                        | [34A] 2              | c7         | c7             | [34A] 2              | c7         | c7             |
| 20   | Record-Route                  | [26] 20.30           | n/a        | c34            | [26] 20.30           | n/a        | c34            |
| 20A  | Recv-Info                     | [25] 5.2.3           | c35        | c35            | [25] 5.2.3           | c35        | c35            |
| 20B  | Referred-By                   | [59] 3               | c16        | c16            | [59] 3               | c17        | c17            |
| 20C  | Reject-Contact                | [56B] 9.2            | c15        | c15            | [56B] 9.2            | c18        | c18            |
| 20D  | Request-Disposition           | [56B] 9.1            | c15        | c15            | [56B] 9.1            | c18        | c18            |
| 21   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | m          | m              |
| 21A  | Resource-Priority             | [116] 3.1            | c33        | c33            | [116] 3.1            | c33        | c33            |
| 22   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | n/a        | c34            |
| 22A  | Session-ID                    | [162]                | o          | c36            | [162]                | o          | c36            |
| 23   | Supported                     | [26] 20.37           | o          | o              | [26] 20.37           | m          | m              |
| 24   | Timestamp                     | [26] 20.38           | c8         | c8             | [26] 20.38           | m          | m              |
| 25   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 26   | User-Agent                    | [26] 20.41           | o          | o              | [26] 20.41           | o          | o              |
| 27   | Via                           | [26] 20.42           | m          | m              | [26] 20.42           | m          | m              |



|      |   |
|------|---|
| c1:  | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.  |
| c2:  | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.  |
| c3:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.  |
| c4:  | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.  |
| c5:  | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.  |
| c6:  | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c7:  | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c8:  | IF A.4/6 THEN o ELSE n/a - - timestamping of requests.  |
| c9:  | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.   |
| c10: | IF A.4/34 AND (A.3/1 OR A.3/2A OR A.3/7 OR A.3A/81) THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE, P-CSCF (IMS-ALG), AS or MSC server enhanced for ICS.   |
| c11: | IF A.4/34 AND (A.3/2A OR A.3A/81 OR A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF (IMS-ALG), MSC server enhanced for ICS, AS acting as terminating UA, AS acting as third-party call controller or EATF.  |
| c12: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.   |
| c13: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c14: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c15: | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.   |
| c16: | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c17: | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.  |
| c18: | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c21: | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network. |
| c22: | IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |
| c33: | IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.   |
| c34: | IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.  |
| c35: | IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.  |
| c36: | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.  |

Prerequisite A.5/14 - - PRACK request

**Table A.92: Supported message bodies within the PRACK request**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

**Table A.93: Void**

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/1 - - Additional for 100 (Trying) response

**Table A.93A: Supported header fields within the PRACK response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID  | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length   | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq   | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date   | [26] 20.17 | c1         | c1             | [26] 20.17 | m          | m              |
| 5    | From   | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To   | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via  | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |            |            |                |            |            |                |

Prerequisite A.5/15 - - PRACK response for all remaining status-codes

**Table A.94: Supported header fields within the PRACK response**

| Item  | Header field   | Sending                          |            |                | Receiving                        |            |                |
|-------|--|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|       |  | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A    | Allow  | [26] 20.5                        | c9         | c9             | [26] 20.5                        | m          | m              |
| 1     | Call-ID  | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 2     | Content-Disposition  | [26] 20.11                       | o          | o              | [26] 20.11                       | m          | m              |
| 3     | Content-Encoding   | [26] 20.12                       | o          | o              | [26] 20.12                       | m          | m              |
| 4     | Content-Language   | [26] 20.13                       | o          | o              | [26] 20.13                       | m          | m              |
| 5     | Content-Length   | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6     | Content-Type   | [26] 20.15                       | m          | m              | [26] 20.15                       | m          | m              |
| 7     | CSeq   | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8     | Date   | [26] 20.17                       | c1         | c1             | [26] 20.17                       | m          | m              |
| 9     | From   | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 10    | MIME-Version   | [26] 20.24                       | o          | o              | [26] 20.24                       | m          | m              |
| 10A   | P-Access-Network-Info  | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c3         | c4             | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c3         | c5             |
| 10B   | P-Charging-Function-Addresses  | [52] 4.5,<br>[52A] 4             | c7         | c8             | [52] 4.5,<br>[52A] 4             | c7         | c8             |
| 10C   | P-Charging-Vector  | [52] 4.6,<br>[52A] 4             | c6         | n/a            | [52] 4.6,<br>[52A] 4             | c6         | n/a            |
| 10E   | P-Early-Media  | [109] 8                          | c10        | c10            | [109] 8                          | c10        | c10            |
| 10F   | Privacy  | [33] 4.2                         | c2         | n/a            | [33] 4.2                         | c2         | n/a            |
| 10G   | Recv-Info  | [25] 5.2.3                       | c13        | c13            | [25] 5.2.3                       | c13        | c13            |
| 10H   | Require  | [26] 20.32                       | m          | m              | [26] 20.32                       | m          | m              |
| 10I   | Server   | [26] 20.35                       | o          | o              | [26] 20.35                       | o          | o              |
| 10J   | Session-ID   | [162]                            | o          | c14            | [162]                            | o          | c14            |
| 11    | Timestamp  | [26] 20.38                       | m          | m              | [26] 20.38                       | c2         | c2             |
| 12    | To   | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 12A   | User-Agent   | [26] 20.41                       | o          | o              | [26] 20.41                       | o          | o              |
| 13    | Via  | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 14    | Warning  | [26] 20.43                       | o (note)   | o              | [26] 20.43                       | o          | o              |
| c1:   | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c2:   | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |                                  |            |                |                                  |            |                |
| c3:   | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.  |                                  |            |                |                                  |            |                |
| c4:   | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.   |                                  |            |                |                                  |            |                |
| c5:   | IF A.4/34 AND (A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA, AS acting as third-party call controller or EATF. |                                  |            |                |                                  |            |                |
| c6:   | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c7:   | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c8:   | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c9:   | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed)   |                                  |            |                |                                  |            |                |
| c10:  | IF A.4/66 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.   |                                  |            |                |                                  |            |                |
| c13:  | IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.   |                                  |            |                |                                  |            |                |
| c14:  | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |
| NOTE: | RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.  |                                  |            |                |                                  |            |                |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.95: Supported header fields within the PRACK response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Accept-Resource-Priority   | [116] 3.2  | c14        | c14            | [116] 3.2  | c14        | c14            |
| 0B   | Allow-Events   | [28] 7.2.2 | c3         | c3             | [28] 7.2.2 | c4         | c4             |
| 0C   | Authentication-Info  | [26] 20.6  | c1         | c1             | [26] 20.6  | c2         | c2             |
| 0D   | P-Early-Media  | [109] 8    | c5         | c5             | [109] 8    | c5         | c5             |
| 3    | Supported  | [26] 20.37 | m          | m              | [26] 20.37 | m          | m              |
| c1:  | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c2:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c3:  | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.                                     |            |            |                |            |            |                |
| c4:  | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.                                   |            |            |                |            |            |                |
| c5:  | IF A.4/66 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media. |            |            |                |            |            |                |
| c14: | IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.            |            |            |                |            |            |                |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.95A: Supported header fields within the PRACK response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | o          | o              | [26] 20.18 | o          | o              |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.96: Supported header fields within the PRACK response**

| Item  | Header field | Sending    |            |                | Receiving  |            |                |
|---|--------------|------------|------------|----------------|------------|------------|----------------|
|   |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1   | Contact      | [26] 20.10 | o (note)   | o              | [26] 20.10 | m          | m              |
| NOTE: RFC 3261 [26] gives the status of this header field as SHOULD rather than OPTIONAL. |              |            |            |                |            |            |                |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.97: Supported header fields within the PRACK response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate  | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 8    | WWW-Authenticate  | [26] 20.44 | m          | m              | [26] 20.44 | m          | m              |
| c1:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response.

**Table A.98: Supported header fields within the PRACK response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | o              |

**Table A.99: Void**

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.100: Supported header fields within the PRACK response**

| Item  | Header field       | Sending    |            |                | Receiving  |            |                |
|---|--------------------|------------|------------|----------------|------------|------------|----------------|
|   |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2   | Proxy-Authenticate | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 6   | WWW-Authenticate   | [26] 20.44 | o          | o              | [26] 20.44 | o          | o              |
| c1: IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |                    |            |            |                |            |            |                |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.101: Supported header fields within the PRACK response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1 | o.1        | o.1            | [26] 20.1 | m          | m              |
| 2    | Accept-Encoding | [26] 20.2 | o.1        | o.1            | [26] 20.2 | m          | m              |
| 3    | Accept-Language | [26] 20.3 | o.1        | o.1            | [26] 20.3 | m          | m              |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.101A: Supported header fields within the PRACK response**

| Item  | Header field             | Sending   |            |                | Receiving |            |                |
|---|--------------------------|-----------|------------|----------------|-----------|------------|----------------|
|   |                          | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1   | Accept-Resource-Priority | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1: IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol. |                          |           |            |                |           |            |                |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.102: Supported header fields within the PRACK response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | m          | m              |

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.102A: Supported header fields within the PRACK response**

| Item  | Header field    | Sending |            |                | Receiving |            |                |
|---|-----------------|---------|------------|----------------|-----------|------------|----------------|
|   |                 | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3   | Security-Server | [48] 2  | x          | x              | [48] 2    | c1         | c1             |
| c1: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |                 |         |            |                |           |            |                |

**Table A.103: Void**

Prerequisite A.5/15 - - PRACK response

**Table A.104: Supported message bodies within the PRACK response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

#### A.2.1.4.10A PUBLISH method

Prerequisite A.5/15A – PUBLISH request

**Table A.104A: Supported header fields within the PUBLISH request**

| Item | Header field                  | Sending                     |            |                | Receiving                   |            |                |
|------|-------------------------------|-----------------------------|------------|----------------|-----------------------------|------------|----------------|
|      |                               | Ref.                        | RFC status | Profile status | Ref.                        | RFC status | Profile status |
| 1    | Accept-Contact                | [56B] 9.2                   | c22        | c22            | [56B] 9.2                   | c28        | c28            |
| 2    | Allow                         | [26] 20.5                   | o          | o              | [26] 20.5                   | m          | m              |
| 3    | Allow-Events                  | [26] 7.2.2                  | c1         | c1             | [26] 7.2.2                  | c2         | c2             |
| 4    | Authorization                 | [26] 20.7                   | c3         | c3             | [26] 20.7                   | c3         | c3             |
| 5    | Call-ID                       | [26] 20.8                   | m          | m              | [26] 20.8                   | m          | m              |
| 6    | Call-Info                     | [26] 20.9                   | o          | o              | [26] 20.9                   | o          | o              |
| 6A   | Contact                       | [26] 20.10                  | o          | o              | [26] 20.10                  | o          | o              |
| 7    | Content-Disposition           | [26] 20.11                  | o          | o              | [26] 20.11                  | m          | m              |
| 8    | Content-Encoding              | [26] 20.12                  | o          | o              | [26] 20.12                  | m          | m              |
| 9    | Content-Language              | [26] 20.13                  | o          | o              | [26] 20.13                  | m          | m              |
| 10   | Content-Length                | [26] 20.14                  | m          | m              | [26] 20.14                  | m          | m              |
| 11   | Content-Type                  | [26] 20.15                  | m          | m              | [26] 20.15                  | m          | m              |
| 12   | CSeq                          | [26] 20.16                  | m          | m              | [26] 20.16                  | m          | m              |
| 13   | Date                          | [26] 20.17                  | c4         | c4             | [26] 20.17                  | m          | m              |
| 14   | Event                         | [70] 4, 6                   | m          | m              | [70] 4, 6                   | m          | m              |
| 15   | Expires                       | [26] 20.19,<br>[70] 4, 5, 6 | o          | o              | [26] 20.19,<br>[70] 4, 5, 6 | m          | m              |
| 15A  | Feature-Caps                  | [190]                       | c41        | c41            | [190]                       | c40        | c40            |
| 16   | From                          | [26] 20.20                  | m          | m              | [26] 20.20                  | m          | m              |
| 16A  | Geolocation                   | [89] 4.1                    | c38        | c38            | [89] 4.1                    | c38        | c38            |
| 16B  | Geolocation-Routing           | [89] 4.2                    | c38        | c38            | [89] 4.2                    | c38        | c38            |
| 16C  | History-Info                  | [66] 4.1                    | c27        | c27            | [66] 4.1                    | c27        | c27            |
| 17   | In-Reply-To                   | [26] 20.21                  | o          | o              | [26] 20.21                  | o          | o              |
| 17A  | Max-Breadth                   | [117] 5.8                   | n/a        | c23            | [117] 5.8                   | c24        | c24            |
| 18   | Max-Forwards                  | [26] 20.22                  | m          | m              | [26] 20.22                  | n/a        | c37            |
| 19   | MIME-Version                  | [26] 20.24                  | o          | o              | [26] 20.24                  | m          | m              |
| 20   | Organization                  | [26] 20.25                  | o          | o              | [26] 20.25                  | o          | o              |
| 21   | P-Access-Network-Info         | [52] 4.4,<br>[234] 2        | c15        | c16            | [52] 4.4,<br>[234] 2        | c15        | c17            |
| 22   | P-Asserted-Identity           | [34] 9.1                    | n/a        | c45            | [34] 9.1                    | c11        | c11            |
| 22A  | P-Asserted-Service            | [121] 4.1                   | n/a        | c46            | [121] 4.1                   | c31        | c31            |
| 23   | P-Called-Party-ID             | [52] 4.2                    | x          | x              | [52] 4.2                    | c13        | c13            |
| 24   | P-Charging-Function-Addresses | [52] 4.5                    | c20        | c21            | [52] 4.5                    | c20        | c21            |
| 25   | P-Charging-Vector             | [52] 4.6                    | c18        | c19            | [52] 4.6                    | c18        | c19            |
| 26   | P-Preferred-Identity          | [34] 9.2                    | c11        | c7             | [34] 9.2                    | n/a        | n/a            |
| 26A  | P-Preferred-Service           | [121] 4.2                   | c31        | c30            | [121] 4.2                   | n/a        | n/a            |
| 26B  | P-Private-Network-Indication  | [134]                       | c33        | c33            | [134]                       | c33        | c33            |
| 26C  | P-Profile-Key                 | [97] 5                      | n/a        | n/a            | [97] 5                      | n/a        | n/a            |
| 26D  | P-Served-User                 | [133] 6                     | c36        | c36            | [133] 6                     | c36        | c36            |
| 26E  | P-User-Database               | [82] 4                      | n/a        | n/a            | [82] 4                      | n/a        | n/a            |
| 27   | P-Visited-Network-ID          | [52] 4.3                    | x (note 3) | x              | [52] 4.3                    | c14        | n/a            |
| 28   | Priority                      | [26] 20.26                  | o          | o              | [26] 20.26                  | o          | o              |
| 29   | Privacy                       | [33] 4.2                    | c12        | c12            | [33] 4.2                    | c12        | c12            |
| 30   | Proxy-Authorization           | [26] 20.28                  | c5         | c5             | [26] 20.28                  | n/a        | n/a            |
| 31   | Proxy-Require                 | [26] 20.29                  | o          | n/a            | [26] 20.29                  | n/a        | n/a            |
| 32   | Reason                        | [34A] 2                     | c8         | c8             | [34A] 2                     | c8         | c8             |
| 33   | Reject-Contact                | [56B] 9.2                   | c22        | c22            | [56B] 9.2                   | c28        | c28            |
| 33A  | Referred-By                   | [59] 3                      | c25        | c25            | [59] 3                      | c26        | c26            |
| 34   | Request-Disposition           | [56B] 9.1                   | c22        | c22            | [56B] 9.1                   | c28        | c28            |
| 35   | Reply-To                      | [26] 20.31                  | o          | o              | [26] 20.31                  | o          | o              |
| 36   | Require                       | [26] 20.32                  | m          | m              | [26] 20.32                  | m          | m              |
| 36A  | Resource-Priority             | [116] 3.1                   | c29        | c29            | [116] 3.1                   | c29        | c29            |
| 37   | Route                         | [26] 20.34                  | m          | m              | [26] 20.34                  | n/a        | c37            |
| 38   | Security-Client               | [48] 2.3.1                  | c9         | c9             | [48] 2.3.1                  | n/a        | n/a            |
| 39   | Security-Verify               | [48] 2.3.1                  | c10        | c10            | [48] 2.3.1                  | n/a        | n/a            |
| 39A  | Session-ID                    | [162]                       | o          | c39            | [162]                       | o          | c39            |
| 40   | SIP-If-Match                  | [70] 11.3.2                 | o          | o              | [70] 11.3.2                 | m          | m              |
| 41   | Subject                       | [26] 20.36                  | o          | o              | [26] 20.36                  | o          | o              |

|  |  |                            |    |    |                            |   |   |
|--|--|----------------------------|----|----|----------------------------|---|---|
| 42   | Supported  | [26]<br>20.37,<br>[26] 7.1 | o  | o  | [26]<br>20.37,<br>[26] 7.1 | m | m |
| 43   | Timestamp  | [26] 20.38                 | c6 | c6 | [26] 20.38                 | m | m |
| 44   | To   | [26] 20.39                 | m  | m  | [26] 20.39                 | m | m |
| 45   | User-Agent   | [26] 20.41                 | o  | o  | [26] 20.41                 | o | o |
| 46   | Via  | [26] 20.42                 | m  | m  | [26] 20.42                 | m | m |
| c1:  | IF A.4/22 THEN o ELSE n/a -- acting as the notifier of event information.  |                            |    |    |                            |   |   |
| c2:  | IF A.4/23 THEN m ELSE n/a -- acting as the subscriber to event information.  |                            |    |    |                            |   |   |
| c3:  | IF A.4/7 THEN m ELSE n/a -- authentication between UA and UA.  |                            |    |    |                            |   |   |
| c4:  | IF A.4/11 THEN o ELSE n/a -- insertion of date in requests and responses.  |                            |    |    |                            |   |   |
| c5:  | IF A.4/8A THEN m ELSE n/a -- authentication between UA and proxy.  |                            |    |    |                            |   |   |
| c6:  | IF A.4/6 THEN o ELSE n/a -- timestamping of requests.  |                            |    |    |                            |   |   |
| c7:  | IF A.3/1 AND A.4/25 THEN o ELSE n/a -- UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.   |                            |    |    |                            |   |   |
| c8:  | IF A.4/38 THEN o ELSE n/a -- the Reason header field for the session initiation protocol.  |                            |    |    |                            |   |   |
| c9:  | IF A.4/37 OR A.4/37A THEN o ELSE n/a -- security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 1).   |                            |    |    |                            |   |   |
| c10:   | IF A.4/37 OR A.4/37A THEN m ELSE n/a -- security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |                            |    |    |                            |   |   |
| c11:   | IF A.4/25 THEN o ELSE n/a -- private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |                            |    |    |                            |   |   |
| c12:   | IF A.4/26 THEN o ELSE n/a -- a privacy mechanism for the Session Initiation Protocol (SIP).  |                            |    |    |                            |   |   |
| c13:   | IF A.4/32 THEN o ELSE n/a -- the P-Called-Party-ID extension.  |                            |    |    |                            |   |   |
| c14:   | IF A.4/33 THEN o ELSE n/a -- the P-Visited-Network-ID extension.   |                            |    |    |                            |   |   |
| c15:   | IF A.4/34 THEN o ELSE n/a -- the P-Access-Network-Info header extension.   |                            |    |    |                            |   |   |
| c16:   | IF A.4/34 AND A.3/1 THEN m ELSE n/a -- the P-Access-Network-Info header extension and UE.  |                            |    |    |                            |   |   |
| c17:   | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a -- the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.  |                            |    |    |                            |   |   |
| c18:   | IF A.4/36 THEN o ELSE n/a -- the P-Charging-Vector header extension.   |                            |    |    |                            |   |   |
| c19:   | IF A.4/36 THEN m ELSE n/a -- the P-Charging-Vector header extension.   |                            |    |    |                            |   |   |
| c20:   | IF A.4/35 THEN o ELSE n/a -- the P-Charging-Function-Addresses header extension.   |                            |    |    |                            |   |   |
| c21:   | IF A.4/35 THEN m ELSE n/a -- the P-Charging-Function-Addresses header extension.   |                            |    |    |                            |   |   |
| c22:   | IF A.4/40 THEN o ELSE n/a -- caller preferences for the session initiation protocol.   |                            |    |    |                            |   |   |
| c23:   | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o -- addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network. |                            |    |    |                            |   |   |
| c24:   | IF A.4/71 THEN m ELSE n/a -- addressing an amplification vulnerability in session initiation protocol forking proxies.   |                            |    |    |                            |   |   |
| c25:   | IF A.4/43 THEN m ELSE n/a -- the SIP Referred-By mechanism.  |                            |    |    |                            |   |   |
| c26:   | IF A.4/43 THEN o ELSE n/a -- the SIP Referred-By mechanism.  |                            |    |    |                            |   |   |
| c27:   | IF A.4/47 THEN m ELSE n/a -- an extension to the session initiation protocol for request history information.  |                            |    |    |                            |   |   |
| c28:   | IF A.4/40 THEN m ELSE n/a -- caller preferences for the session initiation protocol.   |                            |    |    |                            |   |   |
| c29:   | IF A.4/70B THEN m ELSE n/a -- inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.  |                            |    |    |                            |   |   |
| c30:   | IF (A.3/1 OR A.3A/81) AND A.4/74 THEN o ELSE n/a -- UE, MSC Server enhanced for ICS and SIP extension for the identification of services.  |                            |    |    |                            |   |   |
| c31:   | IF A.4/74 THEN o ELSE n/a -- SIP extension for the identification of services.   |                            |    |    |                            |   |   |
| c32:   | IF A.4/74 THEN m ELSE n/a -- SIP extension for the identification of services.   |                            |    |    |                            |   |   |
| c33:   | IF A.4/77 THEN m ELSE n/a -- the SIP P-Private-Network-Indication private-header (P-Header).   |                            |    |    |                            |   |   |
| c36:   | IF A.4/78 THEN m ELSE n/a -- the SIP P-Served-User private header.   |                            |    |    |                            |   |   |
| c37:   | IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o -- UE, UE performing the functions of an external attached network.  |                            |    |    |                            |   |   |
| c38:   | IF A.4/60 THEN m ELSE n/a -- SIP location conveyance.  |                            |    |    |                            |   |   |
| c39:   | IF A.4/91 THEN m ELSE n/a -- the Session-ID header.  |                            |    |    |                            |   |   |
| c40:   | IF A.4/100 THEN m ELSE n/a -- indication of features supported by proxy.   |                            |    |    |                            |   |   |
| c41:   | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a -- indication of features supported by proxy, UE, UE performing the functions of an external attached network.  |                            |    |    |                            |   |   |
| c45:   | IF A.4/25 AND (A.3/7B OR A.3/8) THEN o ELSE n/a -- private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and AS acting as originating UA, MRFC.  |                            |    |    |                            |   |   |
| c46:   | IF A.4/74 AND A.3/7B THEN o ELSE n/a -- SIP extension for the identification of services and AS acting as originating UA.  |                            |    |    |                            |   |   |
| NOTE 1: Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. |  |                            |    |    |                            |   |   |
| NOTE 2: The strength of this requirement in RFC 7315 [52] is SHOULD NOT, rather than MUST NOT.   |  |                            |    |    |                            |   |   |



Prerequisite A.5/15A - - PUBLISH request

**Table A.104B: Supported message bodies within the PUBLISH request**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/1 - - Additional for 100 (Trying) response

**Table A.104BA: Supported header fields within the PUBLISH response**

| Item | Header field   | Sending  |            |                | Receiving  |            |                |
|------|----------------|--|------------|----------------|------------|------------|----------------|
|      |                | Ref.   | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID        | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length | [26] 20.14   | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq           | [26] 20.16   | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date           | [26] 20.17   | c1         | c1             | [26] 20.17 | m          | m              |
| 5    | From           | [26] 20.20   | m          | m              | [26] 20.20 | m          | m              |
| 6    | To             | [26] 20.39   | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via            | [26] 20.42   | m          | m              | [26] 20.42 | m          | m              |
| c1:  |                | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |            |                |            |            |                |

Prerequisite A.5/15B - - PUBLISH response for all remaining status-codes

**Table A.104C: Supported header fields within the PUBLISH response**

| Item  | Header field   | Sending                          |            |                | Receiving                        |            |                |
|-------|--|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|       |  | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A    | Allow  | [26] 20.5                        | c12        | c12            | [26] 20.5                        | m          | m              |
| 1     | Call-ID  | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 2     | Call-Info  | [26] 24.9                        | o          | o              | [26] 24.9                        | m          | m              |
| 3     | Content-Disposition  | [26] 20.11                       | o          | o              | [26] 20.11                       | m          | m              |
| 4     | Content-Encoding   | [26] 20.12                       | o          | o              | [26] 20.12                       | m          | m              |
| 5     | Content-Language   | [26] 20.13                       | o          | o              | [26] 20.13                       | m          | m              |
| 6     | Content-Length   | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 7     | Content-Type   | [26] 20.15                       | m          | m              | [26] 20.15                       | m          | m              |
| 8     | CSeq   | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 9     | Date   | [26] 20.17                       | c1         | c1             | [26] 20.17                       | m          | m              |
| 10    | From   | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 10A   | Geolocation-Error  | [89] 4.3                         | c16        | c16            | [89] 4.3                         | c16        | c16            |
| 10B   | History-Info   | [66] 4.1                         | c13        | c13            | [66] 4.1                         | c13        | c13            |
| 11    | MIME-Version   | [26] 20.24                       | o          | o              | [26] 20.24                       | m          | m              |
| 12    | Organization   | [26] 20.25                       | o          | o              | [26] 20.25                       | o          | o              |
| 13    | P-Access-Network-Info  | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c6             | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c7             |
| 14    | P-Asserted-Identity  | [34] 9.1                         | n/a        | c21            | [34] 9.1                         | c3         | c3             |
| 15    | P-Charging-Function-Addresses  | [52] 4.5,<br>[52A] 4             | c10        | c11            | [52] 4.5,<br>[52A] 4             | c10        | c11            |
| 16    | P-Charging-Vector  | [52] 4.6,<br>[52A] 4             | c8         | c9             | [52] 4.6,<br>[52A] 4             | c8         | c9             |
| 17    | P-Preferred-Identity   | [34] 9.2                         | c3         | x              | [34] 9.2                         | n/a        | n/a            |
| 18    | Privacy  | [33] 4.2                         | c4         | c4             | [33] 4.2                         | c4         | c4             |
| 19    | Require  | [26] 20.32                       | m          | m              | [26] 20.32                       | m          | m              |
| 20    | Server   | [26] 20.35                       | o          | o              | [26] 20.35                       | o          | o              |
| 20A   | Session-ID   | [162]                            | o          | c17            | [162]                            | o          | c17            |
| 21    | Timestamp  | [26] 20.38                       | m          | m              | [26] 20.38                       | c2         | c2             |
| 22    | To   | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 23    | User-Agent   | [26] 20.41                       | o          | o              | [26] 20.41                       | o          | o              |
| 24    | Via  | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 25    | Warning  | [26] 20.43                       | o          | o              | [26] 20.43                       | o          | o              |
| c1:   | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c2:   | IF A.4/6 THEN m ELSE n/a - - timestamping of requests.   |                                  |            |                |                                  |            |                |
| c3:   | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.   |                                  |            |                |                                  |            |                |
| c4:   | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |                                  |            |                |                                  |            |                |
| c5:   | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.  |                                  |            |                |                                  |            |                |
| c6:   | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.   |                                  |            |                |                                  |            |                |
| c7:   | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.                         |                                  |            |                |                                  |            |                |
| c8:   | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c9:   | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c10:  | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c11:  | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c12:  | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).  |                                  |            |                |                                  |            |                |
| c13:  | IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.   |                                  |            |                |                                  |            |                |
| c16:  | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.   |                                  |            |                |                                  |            |                |
| c17:  | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |
| c21:  | IF A.4/25 AND (A.3/7B OR A.3/8) THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and AS acting as originating UA, MRFC. |                                  |            |                |                                  |            |                |
| NOTE: | For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header field as SHOULD rather than OPTIONAL.  |                                  |            |                |                                  |            |                |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/7 - - Additional for 200 (OK) response

**Table A.104D: Supported header fields within the PUBLISH response**

| Item | Header field   | Sending                        |            |                | Receiving                      |            |                |
|------|--|--------------------------------|------------|----------------|--------------------------------|------------|----------------|
|      |  | Ref.                           | RFC status | Profile status | Ref.                           | RFC status | Profile status |
| 1    | Accept-Resource-Priority   | [116] 3.2                      | c3         | c3             | [116] 3.2                      | c3         | c3             |
| 1A   | Allow-Events   | [28] 7.2.2                     | c4         | c4             | [28] 7.2.2                     | c5         | c5             |
| 2    | Authentication-Info  | [26] 20.6                      | c1         | c1             | [26] 20.6                      | c2         | c2             |
| 3    | Expires  | [26] 20.19,<br>[70] 4, 5,<br>6 | m          | m              | [26] 20.19,<br>[70] 4, 5,<br>6 | m          | m              |
| 3A   | Feature-Caps   | [190]                          | c8         | c8             | [190]                          | c7         | c7             |
| 4    | SIP-Etag   | [70] 11.3.1                    | m          | m              | [70] 11.3.1                    | m          | m              |
| 5    | Supported  | [26] 20.37                     | m          | m              | [26] 20.37                     | m          | m              |
| c1:  | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.   |                                |            |                |                                |            |                |
| c2:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.   |                                |            |                |                                |            |                |
| c3:  | IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.                                       |                                |            |                |                                |            |                |
| c4:  | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.   |                                |            |                |                                |            |                |
| c5:  | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.   |                                |            |                |                                |            |                |
| c7:  | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.  |                                |            |                |                                |            |                |
| c8:  | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network. |                                |            |                |                                |            |                |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.104DA: Supported header fields within the PUBLISH response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | o          | o              | [26] 20.18 | o          | o              |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.104E: Supported header fields within the PUBLISH response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Contact      | [26] 20.10 | o          | o              | [26] 20.10 | m          | m              |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 – Additional for 401 (Unauthorized) response

**Table A.104F: Supported header fields within the PUBLISH response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Proxy-Authenticate  | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 5    | WWW-Authenticate  | [26] 20.44 | m          | m              | [26] 20.44 | m          | m              |
| c1:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.104G: Supported header fields within the PUBLISH response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | o              |

**Table A.104H: Void**

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.104I: Supported header fields within the PUBLISH response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Proxy-Authenticate  | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 5    | WWW-Authenticate  | [26] 20.44 | o          | o              | [26] 20.44 | o          | o              |
| c1:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.104J: Supported header fields within the PUBLISH response**

| Item | Header field                                     | Sending   |            |                | Receiving |            |                |
|------|--|-----------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept   | [26] 20.1 | o.1        | o.1            | [26] 20.1 | m          | m              |
| 2    | Accept-Encoding                                  | [26] 20.2 | o.1        | o.1            | [26] 20.2 | m          | m              |
| 3    | Accept-Language                                  | [26] 20.3 | o.1        | o.1            | [26] 20.3 | m          | m              |
| o.1  | At least one of these capabilities is supported. |           |            |                |           |            |                |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.104JA: Supported header fields within the PUBLISH response**

| Item | Header field   | Sending   |            |                | Receiving |            |                |
|------|--|-----------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority   | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.104K: Supported header fields within the PUBLISH response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | m          | m              |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.104L: Supported header fields within the PUBLISH response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | x          | x              | [48] 2    | c1         | c1             |
| c1:  | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/29 - - Additional for 423 (Interval Too Brief) response

**Table A.104M: Supported header fields within the PUBLISH response**

| Item | Header field | Sending                  |            |                | Receiving                |            |                |
|------|--------------|--------------------------|------------|----------------|--------------------------|------------|----------------|
|      |              | Ref.                     | RFC status | Profile status | Ref.                     | RFC status | Profile status |
| 3    | Min-Expires  | [26] 20.23,<br>[70] 5, 6 | m          | m              | [26] 20.23,<br>[70] 5, 6 | m          | m              |

**Table A.104N: Void**

Prerequisite A.5/15B - - PUBLISH response

Prerequisite: A.6/39 - - Additional for 489 (Bad Event) response

**Table A.104O: Supported header fields within the PUBLISH response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Allow-Events | [28] 8.2.2 | m          | m              | [28] 8.2.2 | m          | m              |

Prerequisite A.5/15B - - PUBLISH response

**Table A.104P: Supported message bodies within the PUBLISH response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

### A.2.1.4.11 REFER method

Prerequisite A.5/16 - - REFER request

**Table A.105: Supported header fields within the REFER request**

| Item | Header field                  | Sending                    |            |                | Receiving                  |            |                |
|------|-------------------------------|----------------------------|------------|----------------|----------------------------|------------|----------------|
|      |                               | Ref.                       | RFC status | Profile status | Ref.                       | RFC status | Profile status |
| 0A   | Accept                        | [26] 20.1                  | o          | o              | [26] 20.1                  | m          | m              |
| 0B   | Accept-Contact                | [56B] 9.2                  | c22        | c22            | [56B] 9.2                  | c25        | c25            |
| 0C   | Accept-Encoding               | [26] 20.2                  | o          | o              | [26] 20.2                  | m          | m              |
| 1    | Accept-Language               | [26] 20.3                  | o          | o              | [26] 20.3                  | m          | m              |
| 1A   | Allow                         | [26] 20.5                  | o          | o              | [26] 20.5                  | m          | m              |
| 2    | Allow-Events                  | [28] 7.2.2                 | c1         | c1             | [28] 7.2.2                 | c2         | c2             |
| 3    | Authorization                 | [26] 20.7                  | c3         | c3             | [26] 20.7                  | c3         | c3             |
| 4    | Call-ID                       | [26] 20.8                  | m          | m              | [26] 20.8                  | m          | m              |
| 5    | Contact                       | [26] 20.10                 | m          | m              | [26] 20.10                 | m          | m              |
| 5A   | Content-Disposition           | [26] 20.11                 | o          | o              | [26] 20.11                 | m          | m              |
| 5B   | Content-Encoding              | [26] 20.12                 | o          | o              | [26] 20.12                 | m          | m              |
| 5C   | Content-Language              | [26] 20.13                 | o          | o              | [26] 20.13                 | m          | m              |
| 6    | Content-Length                | [26] 20.14                 | m          | m              | [26] 20.14                 | m          | m              |
| 7    | Content-Type                  | [26] 20.15                 | m          | m              | [26] 20.15                 | m          | m              |
| 8    | CSeq                          | [26] 20.16                 | m          | m              | [26] 20.16                 | m          | m              |
| 9    | Date                          | [26] 20.17                 | c4         | c4             | [26] 20.17                 | m          | m              |
| 10   | Expires                       | [26] 20.19                 | o          | o              | [26] 20.19                 | o          | o              |
| 10A  | Feature-Caps                  | [190]                      | c46        | c46            | [190]                      | c45        | c45            |
| 11   | From                          | [26] 20.20                 | m          | m              | [26] 20.20                 | m          | m              |
| 11A  | Geolocation                   | [89] 4.1                   | c26        | c26            | [89] 4.1                   | c26        | c26            |
| 11B  | Geolocation-Routing           | [89] 4.2                   | c26        | c26            | [89] 4.2                   | c26        | c26            |
| 11C  | History-Info                  | [66] 4.1                   | c24        | c24            | [66] 4.1                   | c24        | c24            |
| 11D  | Max-Breadth                   | [117] 5.8                  | n/a        | c30            | [117] 5.8                  | c31        | c31            |
| 12   | Max-Forwards                  | [26] 20.22                 | m          | m              | [26] 20.22                 | n/a        | c39            |
| 13   | MIME-Version                  | [26] 20.24                 | o          | o              | [26] 20.24                 | m          | m              |
| 14   | Organization                  | [26] 20.25                 | o          | o              | [26] 20.25                 | o          | o              |
| 14A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2       | c12        | c13            | [52] 4.4,<br>[234] 2       | c12        | c14            |
| 14B  | P-Asserted-Identity           | [34] 9.1                   | n/a        | c50            | [34] 9.1                   | c8         | c8             |
| 14C  | P-Asserted-Service            | [121] 4.1                  | n/a        | c51            | [121] 4.1                  | c29        | c29            |
| 14D  | P-Called-Party-ID             | [52] 4.2,<br>[52A] 4       | x          | x              | [52] 4.2,<br>[52A] 4       | c10        | c10            |
| 14E  | P-Charging-Function-Addresses | [52] 4.5                   | c17        | c18            | [52] 4.5                   | c17        | c18            |
| 14F  | P-Charging-Vector             | [52] 4.6                   | c15        | c16            | [52] 4.6                   | c15        | c16            |
| 14H  | P-Preferred-Identity          | [34] 9.2                   | c8         | c7             | [34] 9.2                   | n/a        | n/a            |
| 14I  | P-Preferred-Service           | [121] 4.2                  | c28        | c27            | [121] 4.2                  | n/a        | n/a            |
| 14J  | P-Private-Network-Indication  | [134]                      | c36        | c36            | [134]                      | c36        | c36            |
| 14K  | P-Profile-Key                 | [97] 5                     | n/a        | n/a            | [97] 5                     | n/a        | n/a            |
| 14L  | P-Served-User                 | [133] 6                    | c41        | c41            | [133] 6                    | c41        | c41            |
| 14M  | P-User-Database               | [82] 4                     | n/a        | n/a            | [82] 4                     | n/a        | n/a            |
| 14N  | P-Visited-Network-ID          | [52] 4.3                   | x (note 1) | x              | [52] 4.3                   | c11        | n/a            |
| 14O  | Privacy                       | [33] 4.2                   | c9         | c9             | [33] 4.2                   | c9         | c9             |
| 15   | Proxy-Authorization           | [26] 20.28                 | c5         | c5             | [26] 20.28                 | n/a        | n/a            |
| 16   | Proxy-Require                 | [26] 20.29                 | o          | n/a            | [26] 20.29                 | n/a        | n/a            |
| 16A  | Reason                        | [34A] 2                    | c21        | c21            | [34A] 2                    | c21        | c21            |
| 17   | Record-Route                  | [26] 20.30                 | n/a        | c39            | [26] 20.30                 | m          | m              |
| 17A  | Refer-Sub                     | [173] 4                    | c40        | c40            | [173] 4                    | c40        | c40            |
| 18   | Refer-To                      | [36] 3                     | m          | m              | [36] 3                     | m          | m              |
| 18A  | Referred-By                   | [59] 3                     | c23        | c23            | [59] 3                     | c23        | c23            |
| 18B  | Reject-Contact                | [56B] 9.2                  | c22        | c22            | [56B] 9.2                  | c25        | c25            |
| 18C  | Request-Disposition           | [56B] 9.1                  | c22        | c22            | [56B] 9.1                  | c25        | c25            |
| 19   | Require                       | [26] 20.32                 | m          | m              | [26] 20.32                 | m          | m              |
| 19A  | Resource-Priority             | [116] 3.1                  | c33        | c33            | [116] 3.1                  | c33        | c33            |
| 20   | Route                         | [26] 20.34                 | m          | m              | [26] 20.34                 | n/a        | c39            |
| 20A  | Security-Client               | [48] 2.3.1                 | c19        | c19            | [48] 2.3.1                 | n/a        | n/a            |
| 20B  | Security-Verify               | [48] 2.3.1                 | c20        | c20            | [48] 2.3.1                 | n/a        | n/a            |
| 20C  | Session-ID                    | [162]                      | o          | c42            | [162]                      | o          | c42            |
| 21   | Supported                     | [26]<br>20.37,<br>[26] 7.1 | o          | o              | [26]<br>20.37,<br>[26] 7.1 | m          | m              |
| 21A  | Target-Dialog                 | [184] 7                    | c43        | c43            | [184] 7                    | c44        | c44            |
| 22   | Timestamp                     | [26] 20.38                 | c6         | c6             | [26] 20.38                 | m          | m              |



|     |                 |                 |     |     |                 |     |     |
|-----|-----------------|-----------------|-----|-----|-----------------|-----|-----|
| 23  | To              | [26] 20.39      | m   | m   | [26] 20.39      | m   | m   |
| 23A | Trigger-Consent | [125]<br>5.11.2 | c34 | c34 | [125]<br>5.11.2 | c35 | c35 |
| 24  | User-Agent      | [26] 20.41      | o   | o   | [26] 20.41      | o   | o   |
| 25  | Via             | [26] 20.42      | m   | m   | [26] 20.42      | m   | m   |

|         |   |
|---------|---|
| c1:     | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.  |
| c2:     | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.  |
| c3:     | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.  |
| c4:     | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.  |
| c5:     | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.  |
| c6:     | IF A.4/6 THEN o ELSE n/a - - timestamping of requests.  |
| c7:     | IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.   |
| c8:     | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c9:     | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c10:    | IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.  |
| c11:    | IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.   |
| c12:    | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.   |
| c13:    | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.  |
| c14:    | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.  |
| c15:    | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.   |
| c16:    | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c17:    | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c18:    | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c19:    | IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 2).   |
| c20:    | IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |
| c21:    | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c22:    | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.   |
| c23:    | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By Mechanism.  |
| c24:    | IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c25:    | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c26:    | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.  |
| c27:    | IF (A.3/1 OR A.3A/81) AND A.4/74 THEN o ELSE n/a - - UE, MSC Server enhanced for ICS and SIP extension for the identification of services.  |
| c28:    | IF A.4/74 THEN o ELSE n/a - - SIP extension for the identification of services.   |
| c29:    | IF A.4/74 THEN m ELSE n/a - - SIP extension for the identification of services.   |
| c30:    | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network. |
| c31:    | IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |
| c33:    | IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.   |
| c34:    | IF A.4/75A THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP.  |
| c35:    | IF A.4/75B THEN m ELSE n/a - - a recipient within the framework for consent-based communications in SIP.  |
| c36:    | IF A.4/77 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).   |
| c39:    | IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.  |
| c40:    | IF A.4/95 THEN m ELSE n/a - - suppression of session initiation protocol REFER method implicit subscription.  |
| c41:    | IF A.4/78 THEN m ELSE n/a - - the SIP P-Served-User private header.   |
| c42:    | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.  |
| c43:    | IF A.4/99 THEN o ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.   |
| c44:    | IF A.4/99 THEN m ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.   |
| c45:    | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.   |
| c46:    | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.  |
| c50:    | IF A.4/25 AND (A.3/7B OR A.3/8) THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and AS acting as originating UA, MRFC.  |
| c51:    | IF A.4/74 AND A.3/7B THEN o ELSE n/a - - SIP extension for the identification of services and AS acting as originating UA.  |
| NOTE 1: | The strength of this requirement in RFC 7315 [52] is SHOULD NOT, rather than MUST NOT.  |
| NOTE 2: | Support of this header field in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header field in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].   |

Prerequisite A.5/16 - - REFER request

**Table A.106: Supported message bodies within the REFER request**

| Item | Header                            | Sending |            |                | Receiving |            |                |
|------|-----------------------------------|---------|------------|----------------|-----------|------------|----------------|
|      |                                   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | application/vnd.3gpp.mid-call+xml | [8M] D  | n/a        | o              | [8M] D    | n/a        | o              |

**Table A.107: Void**

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/1 - - Additional for 100 (Trying) response

**Table A.107A: Supported header fields within the REFER response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID  | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length   | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq   | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date   | [26] 20.17 | c1         | c1             | [26] 20.17 | m          | m              |
| 5    | From   | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To   | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via  | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |            |            |                |            |            |                |

Prerequisite A.5/17 - - REFER response for all remaining status-codes

**Table A.108: Supported header fields within the REFER response**

| Item  | Header field   | Sending                          |            |                | Receiving                        |            |                |
|-------|--|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|       |  | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A    | Allow  | [26] 20.5                        | c12        | c12            | [26] 20.5                        | m          | m              |
| 1     | Call-ID  | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 1A    | Contact  | [26] 20.10                       | c13        | c13            | [26] 20.10                       | m          | m              |
| 1B    | Content-Disposition  | [26] 20.11                       | o          | o              | [26] 20.11                       | m          | m              |
| 2     | Content-Encoding   | [26] 20.12                       | o          | o              | [26] 20.12                       | m          | m              |
| 3     | Content-Language   | [26] 20.13                       | o          | o              | [26] 20.13                       | m          | m              |
| 4     | Content-Length   | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 5     | Content-Type   | [26] 20.15                       | m          | m              | [26] 20.15                       | m          | m              |
| 6     | CSeq   | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 7     | Date   | [26] 20.17                       | c1         | c1             | [26] 20.17                       | m          | m              |
| 8     | From   | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 8A    | Geolocation-Error  | [89] 4.3                         | c15        | c15            | [89] 4.3                         | c15        | c15            |
| 8B    | History-Info   | [66] 4.1                         | c14        | c14            | [66] 4.1                         | c14        | c14            |
| 9     | MIME-Version   | [26] 20.24                       | o          | o              | [26] 20.24                       | m          | m              |
| 10    | Organization   | [26] 20.25                       | o          | o              | [26] 20.25                       | o          | o              |
| 10A   | P-Access-Network-Info  | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c6             | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c7             |
| 10B   | P-Asserted-Identity  | [34] 9.1                         | n/a        | c22            | [34] 9.1                         | c3         | c3             |
| 10C   | P-Charging-Function-Addresses  | [52] 4.5,<br>[52A] 4             | c10        | c11            | [52] 4.5,<br>[52A] 4             | c10        | c11            |
| 10D   | P-Charging-Vector  | [52] 4.6,<br>[52A] 4             | c8         | c9             | [52] 4.6,<br>[52A] 4             | c8         | c9             |
| 10F   | P-Preferred-Identity   | [34] 9.2                         | c3         | x              | [34] 9.2                         | n/a        | n/a            |
| 10G   | Privacy  | [33] 4.2                         | c4         | c4             | [33] 4.2                         | c4         | c4             |
| 10H   | Require  | [26] 20.32                       | m          | m              | [26] 20.32                       | m          | m              |
| 10I   | Server   | [26] 20.35                       | o          | o              | [26] 20.35                       | o          | o              |
| 10J   | Session-ID   | [162]                            | o          | c18            | [162]                            | o          | c18            |
| 11    | Timestamp  | [26] 20.38                       | m          | m              | [26] 20.38                       | c2         | c2             |
| 12    | To   | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 12A   | User-Agent   | [26] 20.41                       | o          | o              | [26] 20.41                       | o          | o              |
| 13    | Via  | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 14    | Warning  | [26] 20.43                       | o (note)   | o              | [26] 20.43                       | o          | o              |
| c1:   | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c2:   | IF A.4/6 THEN m ELSE n/a - - timestamping of requests.   |                                  |            |                |                                  |            |                |
| c3:   | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.   |                                  |            |                |                                  |            |                |
| c4:   | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |                                  |            |                |                                  |            |                |
| c5:   | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.  |                                  |            |                |                                  |            |                |
| c6:   | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.   |                                  |            |                |                                  |            |                |
| c7:   | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.                         |                                  |            |                |                                  |            |                |
| c8:   | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c9:   | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c10:  | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c11:  | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c12:  | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed)   |                                  |            |                |                                  |            |                |
| c13:  | IF A.6/102 THEN m ELSE o - - 2xx response.   |                                  |            |                |                                  |            |                |
| c14:  | IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.   |                                  |            |                |                                  |            |                |
| c15:  | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.   |                                  |            |                |                                  |            |                |
| c18:  | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |
| c22:  | IF A.4/25 AND (A.3/7B OR A.3/8) THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and AS acting as originating UA, MRFC. |                                  |            |                |                                  |            |                |
| NOTE: | For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header field as SHOULD rather than OPTIONAL.  |                                  |            |                |                                  |            |                |

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.109: Supported header fields within the REFER response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Accept-Resource-Priority   | [116] 3.2  | c12        | c12            | [116] 3.2  | c12        | c12            |
| 1    | Allow-Events   | [28] 7.2.2 | c3         | c3             | [28] 7.2.2 | c4         | c4             |
| 2    | Authentication-Info  | [26] 20.6  | c1         | c1             | [26] 20.6  | c2         | c2             |
| 3    | Feature-Caps   | [190]      | c15        | c15            | [190]      | c14        | c14            |
| 5    | Record-Route   | [26] 20.30 | m          | m              | [26] 20.30 | m          | m              |
| 6    | Refer-Sub  | [173] 4    | c13        | c13            | [173] 4    | c13        | c13            |
| 8    | Supported  | [26] 20.37 | m          | m              | [26] 20.37 | m          | m              |
| c1:  | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c2:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c3:  | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.   |            |            |                |            |            |                |
| c4:  | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.   |            |            |                |            |            |                |
| c12: | IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.  |            |            |                |            |            |                |
| c13: | IF A.4/95 THEN m ELSE n/a - - suppression of session initiation protocol REFER method implicit subscription.   |            |            |                |            |            |                |
| c14: | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.  |            |            |                |            |            |                |
| c15: | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network. |            |            |                |            |            |                |

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.109A: Supported header fields within the REFER response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | o          | o              | [26] 20.18 | o          | o              |

**Table A.110: Void**

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.111: Supported header fields within the REFER response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Proxy-Authenticate  | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 10   | WWW-Authenticate  | [26] 20.44 | m          | m              | [26] 20.44 | m          | m              |
| c1:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.112: Supported header fields within the REFER response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 6    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | o              |

**Table A.113: Void**

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.114: Supported header fields within the REFER response**

| Item  | Header field       | Sending    |            |                | Receiving  |            |                |
|---|--------------------|------------|------------|----------------|------------|------------|----------------|
|   |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4   | Proxy-Authenticate | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 8   | WWW-Authenticate   | [26] 20.44 | o          | o              | [26] 20.44 | o          | o              |
| c1: IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |                    |            |            |                |            |            |                |

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.115: Supported header fields within the REFER response**

| Item   | Header field    | Sending   |            |                | Receiving |            |                |
|--|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|  |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1  | Accept          | [26] 20.1 | o.1        | o.1            | [26] 20.1 | m          | m              |
| 2  | Accept-Encoding | [26] 20.2 | o.1        | o.1            | [26] 20.2 | m          | m              |
| 3  | Accept-Language | [26] 20.3 | o.1        | o.1            | [26] 20.3 | m          | m              |
| o.1 At least one of these capabilities is supported. |                 |           |            |                |           |            |                |

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.115A: Supported header fields within the REFER response**

| Item  | Header field             | Sending   |            |                | Receiving |            |                |
|---|--------------------------|-----------|------------|----------------|-----------|------------|----------------|
|   |                          | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1   | Accept-Resource-Priority | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1: IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol. |                          |           |            |                |           |            |                |

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.116: Supported header fields within the REFER response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 8    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | m          | m              |

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.116A: Supported header fields within the REFER response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | x          | x              | [48] 2    | c1         | c1             |
| c1:  | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

**Table A.117: Void**

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/29H - - Additional for 470 (Consent Needed) response

**Table A.117A: Supported header fields within the REFER response**

| Item | Header field       | Sending        |            |                | Receiving      |            |                |
|------|--------------------|----------------|------------|----------------|----------------|------------|----------------|
|      |                    | Ref.           | RFC status | Profile status | Ref.           | RFC status | Profile status |
| 1    | Permission-Missing | [125]<br>5.9.3 | m          | m              | [125]<br>5.9.3 | m          | m              |

Prerequisite A.5/17 - - REFER response

**Table A.118: Supported message bodies within the REFER response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

#### A.2.1.4.12 REGISTER method

Prerequisite A.5/18 - - REGISTER request

**Table A.119: Supported header fields within the REGISTER request**



| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | o          | o              | [26] 20.1            | m          | m              |
| 2    | Accept-Encoding               | [26] 20.2            | o          | o              | [26] 20.2            | m          | m              |
| 3    | Accept-Language               | [26] 20.3            | o          | o              | [26] 20.3            | m          | m              |
| 3A   | Allow                         | [26] 20.5            | o          | o              | [26] 20.5            | m          | m              |
| 4    | Allow-Events                  | [28] 7.2.2           | c27        | c27            | [28] 7.2.2           | c1         | c1             |
| 5    | Authorization                 | [26] 20.7,<br>[49]   | c2         | c29            | [26] 20.7,<br>[49]   | m          | c22            |
| 6    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 7    | Call-Info                     | [26] 20.9            | o          | o              | [26] 20.9            | o          | o              |
| 8    | Contact                       | [26] 20.10           | o          | m              | [26] 20.10           | m          | m              |
| 9    | Content-Disposition           | [26] 20.11           | o          | o              | [26] 20.11           | m          | m              |
| 10   | Content-Encoding              | [26] 20.12           | o          | o              | [26] 20.12           | m          | m              |
| 11   | Content-Language              | [26] 20.13           | o          | o              | [26] 20.13           | m          | m              |
| 12   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 13   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | m          | m              |
| 14   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 15   | Date                          | [26] 20.17           | c3         | c3             | [26] 20.17           | m          | m              |
| 16   | Expires                       | [26] 20.19           | o          | o              | [26] 20.19           | m          | m              |
| 16A  | Feature-Caps                  | [190]                | c40        | c40            | [190]                | c39        | c39            |
| 17   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 17A  | Geolocation                   | [89] 4.1             | c31        | c31            | [89] 4.1             | c31        | c31            |
| 17B  | Geolocation-Routing           | [89] 4.2             | c31        | c31            | [89] 4.2             | c31        | c31            |
| 17C  | History-Info                  | [66] 4.1             | c28        | c28            | [66] 4.1             | c28        | c28            |
| 17D  | Max-Breadth                   | [117] 5.8            | n/a        | c35            | [117] 5.8            | c36        | c36            |
| 18   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | n/a        | n/a            |
| 19   | MIME-Version                  | [26] 20.24           | o          | o              | [26] 20.24           | m          | m              |
| 20   | Organization                  | [26] 20.25           | o          | o              | [26] 20.25           | o          | o              |
| 20A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c12        | c13            | [52] 4.4,<br>[234] 2 | c12        | c14            |
| 20B  | P-Charging-Function-Addresses | [52] 4.5             | c17        | c18            | [52] 4.5             | c17        | c18            |
| 20C  | P-Charging-Vector             | [52] 4.6             | c15        | c16            | [52] 4.6             | c15        | c16            |
| 20E  | P-User-Database               | [82] 4               | n/a        | n/a            | [82] 4               | c30        | c30            |
| 20F  | P-Visited-Network-ID          | [52] 4.3             | x (note 2) | x              | [52] 4.3             | c10        | c11            |
| 20G  | Path                          | [35] 4               | c4         | c5             | [35] 4               | m          | c6             |
| 20H  | Privacy                       | [33] 4.2             | c9         | n/a            | [33] 4.2             | c9         | n/a            |
| 21   | Proxy-Authorization           | [26] 20.28           | c8         | c8             | [26] 20.28           | n/a        | n/a            |
| 22   | Proxy-Require                 | [26] 20.29           | o          | o (note 1)     | [26] 20.29           | n/a        | n/a            |
| 22A  | Reason                        | [34A] 2              | c23        | c23            | [34A] 2              | c23        | c23            |
| 22B  | Recv-Info                     | [25] 5.2.3           | c37        | c37            | [25] 5.2.3           | c37        | c37            |
| 22C  | Referred-By                   | [59] 3               | c25        | c25            | [59] 3               | c26        | c26            |
| 22D  | Request-Disposition           | [56B] 9.1            | c24        | c24            | [56B] 9.1            | n/a        | n/a            |
| 23   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | m          | m              |
| 23A  | Resource-Priority             | [116] 3.1            | c32        | c32            | [116] 3.1            | c32        | c32            |
| 24   | Route                         | [26] 20.34           | o          | n/a            | [26] 20.34           | n/a        | n/a            |
| 24A  | Security-Client               | [48] 2.3.1           | c19        | c20            | [48] 2.3.1           | n/a        | n/a            |
| 24B  | Security-Verify               | [48] 2.3.1           | c20        | c20            | [48] 2.3.1           | c21        | n/a            |
| 24C  | Session-ID                    | [162]                | o          | c38            | [162]                | o          | c38            |
| 25   | Supported                     | [26] 20.37           | o          | c29            | [26] 20.37           | m          | m              |
| 26   | Timestamp                     | [26] 20.38           | c7         | c7             | [26] 20.38           | c7         | c7             |
| 27   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 28   | User-Agent                    | [26] 20.41           | o          | o              | [26] 20.41           | o          | o              |
| 29   | Via                           | [26] 20.42           | m          | m              | [26] 20.42           | m          | m              |

|         |   |
|---------|---|
| c1:     | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.  |
| c2:     | IF A.4/8 THEN m ELSE n/a - - authentication between UA and registrar.   |
| c3:     | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.  |
| c4:     | IF A.4/24 THEN o ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.   |
| c5:     | IF A.4/24 THEN x ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.   |
| c6:     | IF A.3/4 THEN m ELSE n/a - - S-CSCF.  |
| c7:     | IF A.4/6 THEN m ELSE n/a - - timestamping of requests.  |
| c8:     | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.  |
| c9:     | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c10:    | IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.   |
| c11:    | IF A.4/33 THEN m ELSE n/a - - the P-Visited-Network-ID extension.   |
| c12:    | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.   |
| c13:    | IF A.4/34 AND (A.3/1 OR A.3/4) THEN o ELSE n/a - - the P-Access-Network-Info header extension and UE or S-CSCF.   |
| c14:    | IF A.4/34 AND (A.3/4 OR A.3/7A) THEN m ELSE n/a - - the P-Access-Network-Info header extension and S-CSCF or AS acting as terminating UA.   |
| c15:    | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.   |
| c16:    | IF A.4/36 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Vector header extension (including S-CSCF as registrar).  |
| c17:    | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c18:    | IF A.4/35 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension (including S-CSCF as registrar).  |
| c19:    | IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 3).   |
| c20:    | IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |
| c21:    | IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar.   |
| c22:    | IF A.3/4 THEN m ELSE n/a - - S-CSCF.  |
| c23:    | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c24:    | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.   |
| c25:    | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c26:    | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.  |
| c27:    | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.  |
| c28:    | IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c29:    | IF (A.3/1 OR A.3A/81) THEN m ELSE o - - UE, MSC Server enhanced for ICS.  |
| c30:    | IF A.4/48 THEN m ELSE n/a - - the P-User-Database private header extension.   |
| c31:    | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.  |
| c32:    | IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.  |
| c35:    | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE n/a - - IF A.4/71 AND (A.3/9B OR A.3/9C) THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling). |
| c36:    | IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |
| c37:    | IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.  |
| c38:    | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.  |
| c39:    | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.   |
| c40:    | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.  |
| NOTE 1: | No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.   |
| NOTE 2: | The strength of this requirement in RFC 7315 [52] is SHOULD NOT, rather than MUST NOT.  |
| NOTE 3: | Support of this header field in this method is dependent on the security mechanism and the security architecture which is implemented.  |

Prerequisite A.5/18 - - REGISTER request

**Table A.120: Supported message bodies within the REGISTER request**

| Item | Header                               | Sending       |            |                | Receiving     |            |                |
|------|--------------------------------------|---------------|------------|----------------|---------------|------------|----------------|
|      |                                      | Ref.          | RFC status | Profile status | Ref.          | RFC status | Profile status |
| 1    | message/sip                          | [26] 27.5     | n/a        | c1             | [26] 27.5     | n/a        | c2             |
| 2    | 3GPP IM CN subsystem XML body        | subclause 7.6 | n/a        | c1             | subclause 7.6 | n/a        | c2             |
| c1:  | IF A.3/4 THEN o ELSE n/a - - S-CSCF. |               |            |                |               |            |                |
| c2:  | IF A.3/7 THEN o ELSE n/a - - AS.     |               |            |                |               |            |                |

**Table A.121: Void**

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/1 - - Additional for 100 (Trying) response

**Table A.121A: Supported header fields within the REGISTER response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID  | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length   | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq   | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date   | [26] 20.17 | c1         | c1             | [26] 20.17 | m          | m              |
| 5    | From   | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To   | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via  | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |            |            |                |            |            |                |

Prerequisite A.5/19 - - REGISTER response for all remaining status-codes

**Table A.122: Supported header fields within the REGISTER response**

| Item  | Header field  | Sending                          |            |                | Receiving                        |            |                |
|-------|---|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|       |   | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A    | Allow   | [26] 20.5                        | c8         | c8             | [26] 20.5                        | m          | m              |
| 1     | Call-ID   | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 1A    | Call-Info   | [26] 20.9                        | o          | o              | [26] 20.9                        | o          | o              |
| 2     | Content-Disposition   | [26] 20.11                       | o          | o              | [26] 20.11                       | m          | m              |
| 3     | Content-Encoding  | [26] 20.12                       | o          | o              | [26] 20.12                       | m          | m              |
| 4     | Content-Language  | [26] 20.13                       | o          | o              | [26] 20.13                       | m          | m              |
| 5     | Content-Length  | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6     | Content-Type  | [26] 20.15                       | m          | m              | [26] 20.15                       | m          | m              |
| 7     | CSeq  | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8     | Date  | [26] 20.17                       | c1         | c1             | [26] 20.17                       | m          | m              |
| 9     | From  | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A    | Geolocation-Error   | [89] 4.3                         | c10        | c10            | [89] 4.3                         | c10        | c10            |
| 9B    | History-Info  | [66] 4.1                         | c9         | c9             | [66] 4.1                         | c9         | c9             |
| 10    | MIME-Version  | [26] 20.24                       | o          | o              | [26] 20.24                       | m          | m              |
| 11    | Organization  | [26] 20.25                       | o          | o              | [26] 20.25                       | o          | o              |
| 11A   | P-Access-Network-Info   | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c3         | n/a            | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c3         | n/a            |
| 11B   | P-Charging-Function-Addresses   | [52] 4.5,<br>[52A] 4             | c6         | c7             | [52] 4.5,<br>[52A] 4             | c6         | c7             |
| 11C   | P-Charging-Vector   | [52] 4.6,<br>[52A] 4             | c4         | c5             | [52] 4.6,<br>[52A] 4             | c4         | c5             |
| 11E   | Privacy   | [33] 4.2                         | c2         | n/a            | [33] 4.2                         | c2         | n/a            |
| 11F   | Require   | [26] 20.32                       | m          | m              | [26] 20.32                       | m          | m              |
| 11G   | Server  | [26] 20.35                       | o          | o              | [26] 20.35                       | o          | o              |
| 11H   | Session-ID  | [162]                            | o          | c13            | [162]                            | o          | c13            |
| 12    | Timestamp   | [26] 20.38                       | c2         | c2             | [26] 20.38                       | m          | m              |
| 13    | To  | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 13A   | User-Agent  | [26] 20.41                       | o          | o              | [26] 20.41                       | o          | o              |
| 14    | Via   | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 15    | Warning   | [26] 20.43                       | o (note)   | o              | [26] 20.43                       | o          | o              |
| c1:   | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.  |                                  |            |                |                                  |            |                |
| c2:   | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).                                  |                                  |            |                |                                  |            |                |
| c3:   | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.   |                                  |            |                |                                  |            |                |
| c4:   | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.   |                                  |            |                |                                  |            |                |
| c5:   | IF A.4/36 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Vector header extension (including S-CSCF as registrar).                |                                  |            |                |                                  |            |                |
| c6:   | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.   |                                  |            |                |                                  |            |                |
| c7:   | IF A.4/35 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension (including S-CSCF as registrar).    |                                  |            |                |                                  |            |                |
| c8:   | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).   |                                  |            |                |                                  |            |                |
| c9:   | IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.                |                                  |            |                |                                  |            |                |
| c10:  | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.  |                                  |            |                |                                  |            |                |
| c13:  | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.  |                                  |            |                |                                  |            |                |
| NOTE: | For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header field as SHOULD rather than OPTIONAL. |                                  |            |                |                                  |            |                |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.123: Supported header fields within the REGISTER response**

| Item | Header field   | Sending          |            |                | Receiving        |            |                |
|------|--|------------------|------------|----------------|------------------|------------|----------------|
|      |  | Ref.             | RFC status | Profile status | Ref.             | RFC status | Profile status |
| 1    | Accept   | [26] 20.1        | o          | o              | [26] 20.1        | o          | o              |
| 1A   | Accept-Encoding  | [26] 20.2        | o          | o              | [26] 20.2        | m          | m              |
| 1B   | Accept-Language  | [26] 20.3        | o          | o              | [26] 20.3        | m          | m              |
| 1C   | Accept-Resource-Priority   | [116] 3.2        | c14        | c14            | [116] 3.2        | c14        | c14            |
| 2    | Allow-Events   | [28] 7.2.2       | c12        | c12            | [28] 7.2.2       | c13        | c13            |
| 3    | Authentication-Info  | [26] 20.6        | c6         | c6             | [26] 20.6        | c7         | c7             |
| 5    | Contact  | [26] 20.10       | o          | o              | [26] 20.10       | m          | m              |
| 5A   | Feature-Caps   | [190]            | c18        | c18            | [190]            | c17        | c17            |
| 5B   | Flow-Timer   | [92] 11          | c15        | c15            | [92] 11          | c15        | c15            |
| 5C   | P-Associated-URI   | [52] 4.1         | c8         | c9             | [52] 4.1         | c10        | c11            |
| 6    | Path   | [35] 4           | c3         | c3             | [35] 4           | c4         | c4             |
| 7    | Security-Server  | Subclause 7.2A.7 | n/a        | x              | Subclause 7.2A.7 | n/a        | c16            |
| 8    | Service-Route  | [38] 5           | c5         | c5             | [38] 5           | c5         | c5             |
| 9    | Supported  | [26] 20.37       | m          | m              | [26] 20.37       | m          | m              |
| c1:  | IF (A.3/4 AND A.4/2) THEN m ELSE n/a - - S-CSCF acting as registrar.   |                  |            |                |                  |            |                |
| c2:  | IF A.3/4 OR A.3/1 THEN m ELSE n/a - - S-CSCF or UE.  |                  |            |                |                  |            |                |
| c3:  | IF A.4/24 THEN m ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.  |                  |            |                |                  |            |                |
| c4:  | IF A.4/24 THEN o ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.  |                  |            |                |                  |            |                |
| c5:  | IF A.4/28 THEN m ELSE n/a - - session initiation protocol extension header field for service route discovery during registration.  |                  |            |                |                  |            |                |
| c6:  | IF A.4/8 THEN o ELSE n/a - - authentication between UA and registrar.  |                  |            |                |                  |            |                |
| c7:  | IF A.4/8 THEN m ELSE n/a - - authentication between UA and registrar.  |                  |            |                |                  |            |                |
| c8:  | IF A.4/2 AND A.4/31 THEN m ELSE n/a - - P-Associated-URI header extension and registrar.   |                  |            |                |                  |            |                |
| c9:  | IF A.3/1 AND A.4/31 THEN m ELSE n/a - - P-Associated-URI header extension and S-CSCF.  |                  |            |                |                  |            |                |
| c10: | IF A.4/31 THEN o ELSE n/a - - P-Associated-URI header extension.   |                  |            |                |                  |            |                |
| c11: | IF A.4/31 AND A.3/1 THEN m ELSE n/a - - P-Associated-URI header extension and UE.  |                  |            |                |                  |            |                |
| c12: | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.   |                  |            |                |                  |            |                |
| c13: | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.   |                  |            |                |                  |            |                |
| c14: | IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.                                       |                  |            |                |                  |            |                |
| c15: | IF A.4/57 THEN m ELSE n/a - - managing client initiated connections in SIP.  |                  |            |                |                  |            |                |
| c16: | IF A.4/37A THEN m ELSE n/a - - mediasec header field parameter for marking security mechanisms related to media.   |                  |            |                |                  |            |                |
| c17: | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.  |                  |            |                |                  |            |                |
| c18: | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network. |                  |            |                |                  |            |                |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.123A: Supported header fields within the REGISTER response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | o          | o              | [26] 20.18 | o          | o              |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.124: Supported header fields within the REGISTER response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Contact      | [26] 20.10 | o (note)   | o              | [26] 20.10 | m          | m              |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.125: Supported header fields within the REGISTER response**

| Item | Header field       | Sending   |            |                | Receiving  |            |                |
|------|--------------------|---|------------|----------------|------------|------------|----------------|
|      |                    | Ref.  | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Proxy-Authenticate | [26] 20.27  | c1         | x              | [26] 20.27 | c1         | x              |
| 6    | Security-Server    | [48] 2  | x          | x              | [48] 2     | n/a        | c2             |
| 10   | WWW-Authenticate   | [26] 20.44  | m          | m              | [26] 20.44 | m          | m              |
| c1:  |                    | IF A.4/8 THEN m ELSE n/a - - support of authentication between UA and registrar.                |            |                |            |            |                |
| c2:  |                    | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |            |                |            |            |                |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.126: Supported header fields within the REGISTER response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 6    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | o              |

**Table A.127: Void**

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.128: Supported header fields within the REGISTER response**

| Item | Header field       | Sending  |            |                | Receiving  |            |                |
|------|--------------------|--|------------|----------------|------------|------------|----------------|
|      |                    | Ref.   | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Proxy-Authenticate | [26] 20.27   | c1         | x              | [26] 20.27 | c1         | x              |
| 9    | WWW-Authenticate   | [26] 20.44   | o          | o              | [26] 20.44 | o          | o              |
| c1:  |                    | IF A.4/8 THEN m ELSE n/a - - support of authentication between UA and registrar. |            |                |            |            |                |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.129: Supported header fields within the REGISTER response**

| Item | Header field    | Sending  |            |                | Receiving |            |                |
|------|-----------------|--|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.   | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1  | o.1        | o.1            | [26] 20.1 | m          | m              |
| 2    | Accept-Encoding | [26] 20.2  | o.1        | o.1            | [26] 20.2 | m          | m              |
| 3    | Accept-Language | [26] 20.3  | o.1        | o.1            | [26] 20.3 | m          | m              |
| o.1  |                 | At least one of these capabilities is supported. |            |                |           |            |                |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.129A: Supported header fields within the REGISTER response**

| Item | Header field             | Sending  |            |                | Receiving |            |                |
|------|--------------------------|--|------------|----------------|-----------|------------|----------------|
|      |                          | Ref.   | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority | [116] 3.2  | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  |                          | IF A.4/70B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol. |            |                |           |            |                |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.130: Supported header fields within the REGISTER response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 8    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | m          | m              |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.130A: Supported header fields within the REGISTER response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | c2         | c2             | [48] 2    | c1         | c1             |
| c1:  | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.                         |         |            |                |           |            |                |
| c2:  | IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar. |         |            |                |           |            |                |

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/29 - - Additional for 423 (Interval Too Brief) response

**Table A.131: Supported header fields within the REGISTER response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Min-Expires  | [26] 20.23 | m          | m              | [26] 20.23 | m          | m              |

**Table A.132: Void**

Prerequisite A.5/19 - - REGISTER response

**Table A.133: Supported message bodies within the REGISTER response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |



### A.2.1.4.13 SUBSCRIBE method

Prerequisite A.5/20 - - SUBSCRIBE request

**Table A.134: Supported header fields within the SUBSCRIBE request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | o          | o              | [26] 20.1            | m          | m              |
| 1A   | Accept-Contact                | [56B] 9.2            | c22        | c22            | [56B] 9.2            | c26        | c26            |
| 2    | Accept-Encoding               | [26] 20.2            | o          | o              | [26] 20.2            | m          | m              |
| 3    | Accept-Language               | [26] 20.3            | o          | o              | [26] 20.3            | m          | m              |
| 3A   | Allow                         | [26] 20.5            | o          | o              | [26] 20.5            | m          | m              |
| 4    | Allow-Events                  | [28] 7.2.2           | o          | o              | [28] 7.2.2           | m          | m              |
| 5    | Authorization                 | [26] 20.7            | c3         | c3             | [26] 20.7            | c3         | c3             |
| 6    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 6A   | Call-Info                     | [26] 20.9            | o          | o              | [26] 20.9            | o          | o              |
| 6B   | Contact                       | [26] 20.10           | m          | m              | [26] 20.10           | m          | m              |
| 7    | Content-Disposition           | [26] 20.11           | o          | o              | [26] 20.11           | m          | m              |
| 8    | Content-Encoding              | [26] 20.12           | o          | o              | [26] 20.12           | m          | m              |
| 9    | Content-Language              | [26] 20.13           | o          | o              | [26] 20.13           | m          | m              |
| 10   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 11   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | m          | m              |
| 12   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 13   | Date                          | [26] 20.17           | c4         | c4             | [26] 20.17           | m          | m              |
| 14   | Event                         | [28] 7.2.1           | m          | m              | [28] 7.2.1           | m          | m              |
| 15   | Expires                       | [26] 20.19           | o (note 1) | o (note 1)     | [26] 20.19           | m          | m              |
| 15A  | Feature-Caps                  | [190]                | c46        | c46            | [190]                | c45        | c45            |
| 16   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 16A  | Geolocation                   | [89] 4.1             | c27        | c27            | [89] 4.1             | c27        | c27            |
| 16B  | Geolocation-Routing           | [89] 4.2             | c27        | c27            | [89] 4.2             | c27        | c27            |
| 16C  | History-Info                  | [66] 4.1             | c25        | c25            | [66] 4.1             | c25        | c25            |
| 16D  | Max-Breadth                   | [117] 5.8            | n/a        | c38            | [117] 5.8            | c39        | c39            |
| 17   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | n/a        | c41            |
| 18   | MIME-Version                  | [26] 20.24           | o          | o              | [26] 20.24           | m          | m              |
| 18A  | Organization                  | [26] 20.25           | o          | o              | [26] 20.25           | o          | o              |
| 18B  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c12        | c13            | [52] 4.4,<br>[234] 2 | c12        | c14            |
| 18C  | P-Asserted-Identity           | [34] 9.1             | n/a        | c50            | [34] 9.1             | c6         | c6             |
| 18D  | P-Asserted-Service            | [121] 4.1            | n/a        | c51            | [121] 4.1            | c32        | c32            |
| 18E  | P-Called-Party-ID             | [52] 4.2             | x          | x              | [52] 4.2             | c10        | c10            |
| 18F  | P-Charging-Function-Addresses | [52] 4.5             | c17        | c18            | [52] 4.5             | c17        | c18            |
| 18G  | P-Charging-Vector             | [52] 4.6             | c15        | c16            | [52] 4.6             | c15        | c16            |
| 18I  | P-Preferred-Identity          | [34] 9.2             | c6         | c7             | [34] 9.2             | n/a        | n/a            |
| 18J  | P-Preferred-Service           | [121] 4.2            | c31        | c30            | [121] 4.2            | n/a        | n/a            |
| 18K  | P-Private-Network-Indication  | [134]                | c35        | c35            | [134]                | c35        | c35            |
| 18L  | P-Profile-Key                 | [97] 5               | n/a        | n/a            | [97] 5               | n/a        | n/a            |
| 18M  | P-Served-User                 | [133] 6              | c40        | c40            | [133] 6              | c40        | c40            |
| 18N  | P-User-Database               | [82] 4               | n/a        | n/a            | [82] 4               | n/a        | n/a            |
| 18O  | P-Visited-Network-ID          | [52] 4.3             | x (note 2) | x              | [52] 4.3             | c11        | n/a            |
| 18P  | Privacy                       | [33] 4.2             | c9         | c9             | [33] 4.2             | c9         | c9             |
| 19   | Proxy-Authorization           | [26] 20.28           | c5         | c5             | [26] 20.28           | n/a        | n/a            |
| 20   | Proxy-Require                 | [26] 20.29           | o          | n/a            | [26] 20.29           | n/a        | n/a            |
| 20A  | Reason                        | [34A] 2              | c21        | c21            | [34A] 2              | c21        | c21            |
| 21   | Record-Route                  | [26] 20.30           | n/a        | c41            | [26] 20.30           | m          | m              |
| 21A  | Referred-By                   | [59] 3               | c23        | c23            | [59] 3               | c24        | c24            |
| 21B  | Reject-Contact                | [56B] 9.2            | c22        | c22            | [56B] 9.2            | c26        | c26            |
| 21C  | Request-Disposition           | [56B] 9.1            | c22        | c22            | [56B] 9.1            | c26        | c26            |
| 22   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | m          | m              |
| 22A  | Resource-Priority             | [116] 3.1            | c29        | c29            | [116] 3.1            | c29        | c29            |
| 23   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | n/a        | c41            |
| 23A  | Security-Client               | [48] 2.3.1           | c19        | c19            | [48] 2.3.1           | n/a        | n/a            |
| 23B  | Security-Verify               | [48] 2.3.1           | c20        | c20            | [48] 2.3.1           | n/a        | n/a            |
| 23C  | Session-ID                    | [162]                | o          | c42            | [162]                | o          | c42            |
| 24   | Supported                     | [26] 20.37           | o          | o              | [26] 20.37           | m          | m              |
| 24A  | Target-Dialog                 | [184] 7              | c43        | c43            | [184] 7              | c44        | c44            |
| 25   | Timestamp                     | [26] 20.38           | c8         | c8             | [26] 20.38           | m          | m              |
| 26   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |

|      |   |                 |     |     |                 |     |     |
|------|---|-----------------|-----|-----|-----------------|-----|-----|
| 26A  | Trigger-Consent   | [125]<br>5.11.2 | c33 | c33 | [125]<br>5.11.2 | c34 | c34 |
| 27   | User-Agent  | [26] 20.41      | o   | o   | [26] 20.41      | o   | o   |
| 28   | Via   | [26] 20.42      | m   | m   | [26] 20.42      | m   | m   |
| c3:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.  |                 |     |     |                 |     |     |
| c4:  | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.  |                 |     |     |                 |     |     |
| c5:  | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.  |                 |     |     |                 |     |     |
| c6:  | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |                 |     |     |                 |     |     |
| c7:  | IF A.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.   |                 |     |     |                 |     |     |
| c8:  | IF A.4/6 THEN o ELSE n/a - - timestamping of requests.  |                 |     |     |                 |     |     |
| c9:  | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |                 |     |     |                 |     |     |
| c10: | IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.  |                 |     |     |                 |     |     |
| c11: | IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.   |                 |     |     |                 |     |     |
| c12: | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.   |                 |     |     |                 |     |     |
| c13: | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.  |                 |     |     |                 |     |     |
| c14: | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.  |                 |     |     |                 |     |     |
| c15: | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.   |                 |     |     |                 |     |     |
| c16: | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |                 |     |     |                 |     |     |
| c17: | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.   |                 |     |     |                 |     |     |
| c18: | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |                 |     |     |                 |     |     |
| c19: | IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 3).   |                 |     |     |                 |     |     |
| c20: | IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |                 |     |     |                 |     |     |
| c21: | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.  |                 |     |     |                 |     |     |
| c22: | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.   |                 |     |     |                 |     |     |
| c23: | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |                 |     |     |                 |     |     |
| c24: | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.  |                 |     |     |                 |     |     |
| c25: | IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |                 |     |     |                 |     |     |
| c26: | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |                 |     |     |                 |     |     |
| c27: | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.  |                 |     |     |                 |     |     |
| c29: | IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.   |                 |     |     |                 |     |     |
| c30: | IF (A.3/1 OR A.3A/81) AND A.4/74 THEN o ELSE n/a - - UE, MSC Server enhanced for ICS and SIP extension for the identification of services.  |                 |     |     |                 |     |     |
| c31: | IF A.4/74 THEN o ELSE n/a - - SIP extension for the identification of services.   |                 |     |     |                 |     |     |
| c32: | IF A.4/74 THEN m ELSE n/a - - SIP extension for the identification of services.   |                 |     |     |                 |     |     |
| c33: | IF A.4/75A THEN m ELSE n/a - - a relay within the framework for consent-based communications in SIP.  |                 |     |     |                 |     |     |
| c34: | IF A.4/75B THEN m ELSE n/a - - a recipient within the framework for consent-based communications in SIP.  |                 |     |     |                 |     |     |
| c35: | IF A.4/77 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).   |                 |     |     |                 |     |     |
| c38: | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network. |                 |     |     |                 |     |     |
| c39: | IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |                 |     |     |                 |     |     |
| c40: | IF A.4/78 THEN m ELSE n/a - - the SIP P-Served-User private header.   |                 |     |     |                 |     |     |
| c41: | IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.  |                 |     |     |                 |     |     |
| c42: | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.  |                 |     |     |                 |     |     |
| c43: | IF A.4/99 THEN o ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.   |                 |     |     |                 |     |     |
| c44: | IF A.4/99 THEN m ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.   |                 |     |     |                 |     |     |
| c45: | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.   |                 |     |     |                 |     |     |
| c46: | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.  |                 |     |     |                 |     |     |
| c50: | IF A.4/25 AND (A.3/7B OR A.3/8 OR A.3A/81) THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and AS acting as originating UA, MRFC, MSC Server enhanced for ICS.  |                 |     |     |                 |     |     |
| c51: | IF A.4/74 AND A.3/7B THEN o ELSE n/a - - SIP extension for the identification of services and AS acting as originating UA.  |                 |     |     |                 |     |     |

NOTE 1: The strength of this requirement is RECOMMENDED rather than OPTIONAL.  
 NOTE 2: The strength of this requirement in RFC 7315 [52] is SHOULD NOT, rather than MUST NOT.  
 NOTE 3: Support of this header field in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header field in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Prerequisite A.5/20 - - SUBSCRIBE request

**Table A.135: Supported message bodies within the SUBSCRIBE request**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/1 - - Additional for 100 (Trying) response

**Table A.135A: Supported header fields within the SUBSCRIBE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID  | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length   | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq   | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date   | [26] 20.17 | c1         | c1             | [26] 20.17 | m          | m              |
| 5    | From   | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To   | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via  | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |            |            |                |            |            |                |

Prerequisite A.5/21 - - SUBSCRIBE response for all remaining status-codes

**Table A.136: Supported header fields within the SUBSCRIBE response**

| Item  | Header field   | Sending                          |            |                | Receiving                        |            |                |
|-------|--|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|       |  | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A    | Allow  | [26] 20.5                        | c12        | c12            | [26] 20.5                        | m          | m              |
| 1     | Call-ID  | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 1A    | Call-Info  | [26] 20.9                        | o          | o              | [26] 20.9                        | o          | o              |
| 2     | Content-Disposition  | [26] 20.11                       | o          | o              | [26] 20.11                       | m          | m              |
| 3     | Content-Encoding   | [26] 20.12                       | o          | o              | [26] 20.12                       | m          | m              |
| 4     | Content-Language   | [26] 20.13                       | o          | o              | [26] 20.13                       | m          | m              |
| 5     | Content-Length   | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6     | Content-Type   | [26] 20.15                       | m          | m              | [26] 20.15                       | m          | m              |
| 7     | CSeq   | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8     | Date   | [26] 20.17                       | c1         | c1             | [26] 20.17                       | m          | m              |
| 9     | From   | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A    | Geolocation-Error  | [89] 4.3                         | c14        | c14            | [89] 4.3                         | c14        | c14            |
| 9B    | History-Info   | [66] 4.1                         | c13        | c13            | [66] 4.1                         | c13        | c13            |
| 10    | MIME-Version   | [26] 20.24                       | o          | o              | [26] 20.24                       | m          | m              |
| 10A   | Organization   | [26] 20.25                       | o          | o              | [26] 20.25                       | o          | o              |
| 10B   | P-Access-Network-Info  | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c6             | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c5         | c7             |
| 10C   | P-Asserted-Identity  | [34] 9.1                         | n/a        | c21            | [34] 9.1                         | c3         | c3             |
| 10D   | P-Charging-Function-Addresses  | [52] 4.5,<br>[52A] 4             | c10        | c11            | [52] 4.5,<br>[52A] 4             | c10        | c11            |
| 10E   | P-Charging-Vector  | [52] 4.6,<br>[52A] 4             | c8         | c9             | [52] 4.6,<br>[52A] 4             | c8         | c9             |
| 10G   | P-Preferred-Identity   | [34] 9.2                         | c3         | x              | [34] 9.2                         | n/a        | n/a            |
| 10H   | Privacy  | [33] 4.2                         | c4         | c4             | [33] 4.2                         | c4         | c4             |
| 10I   | Require  | [26] 20.32                       | m          | m              | [26] 20.32                       | m          | m              |
| 10J   | Server   | [26] 20.35                       | o          | o              | [26] 20.35                       | o          | o              |
| 10K   | Session-ID   | [162]                            | o          | c17            | [162]                            | o          | c17            |
| 11    | Timestamp  | [26] 20.38                       | m          | m              | [26] 20.38                       | c2         | c2             |
| 12    | To   | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 12A   | User-Agent   | [26] 20.41                       | o          | o              | [26] 20.41                       | o          | o              |
| 13    | Via  | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 14    | Warning  | [26] 20.43                       | o (note)   | o              | [26] 20.43                       | o          | o              |
| c1:   | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c2:   | IF A.4/6 THEN m ELSE n/a - - timestamping of requests.   |                                  |            |                |                                  |            |                |
| c3:   | IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.   |                                  |            |                |                                  |            |                |
| c4:   | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |                                  |            |                |                                  |            |                |
| c5:   | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.  |                                  |            |                |                                  |            |                |
| c6:   | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.   |                                  |            |                |                                  |            |                |
| c7:   | IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.                         |                                  |            |                |                                  |            |                |
| c8:   | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c9:   | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c10:  | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c11:  | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c12:  | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).  |                                  |            |                |                                  |            |                |
| c13:  | IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.   |                                  |            |                |                                  |            |                |
| c14:  | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.   |                                  |            |                |                                  |            |                |
| c17:  | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |
| c21:  | IF A.4/25 AND (A.3/7B OR A.3/8) THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks and AS acting as originating UA, MRFC. |                                  |            |                |                                  |            |                |
| NOTE: | For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header field as SHOULD rather than OPTIONAL.  |                                  |            |                |                                  |            |                |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.137: Supported header fields within the SUBSCRIBE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Accept-Resource-Priority   | [116] 3.2  | c5         | c5             | [116] 3.2  | c5         | c5             |
| 0B   | Allow-Events   | [28] 7.2.2 | o          | o              | [28] 7.2.2 | m          | m              |
| 1    | Authentication-Info  | [26] 20.6  | c1         | c1             | [26] 20.6  | c2         | c2             |
| 1A   | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | m          | m              |
| 2    | Expires  | [26] 20.19 | m          | m              | [26] 20.19 | m          | m              |
| 2A   | Feature-Caps   | [190]      | c8         | c8             | [190]      | c7         | c7             |
| 3    | Record-Route   | [26] 20.30 | m          | m              | [26] 20.30 | m          | m              |
| 4    | Require  | [26] 20.32 | m          | m              | [26] 20.32 | m          | m              |
| 6    | Supported  | [26] 20.37 | m          | m              | [26] 20.37 | m          | m              |
| c1:  | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c2:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c5:  | IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.  |            |            |                |            |            |                |
| c7:  | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.  |            |            |                |            |            |                |
| c8:  | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network. |            |            |                |            |            |                |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.137A: Supported header fields within the SUBSCRIBE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | o          | o              | [26] 20.18 | o          | o              |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.138: Supported header fields within the SUBSCRIBE response**

| Item  | Header field | Sending    |            |                | Receiving  |            |                |
|---|--------------|------------|------------|----------------|------------|------------|----------------|
|   |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1   | Contact      | [26] 20.10 | m (note)   | m              | [26] 20.10 | m          | m              |
| NOTE: The strength of this requirement is RECOMMENDED rather than MANDATORY for a 485 response. |              |            |            |                |            |            |                |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.139: Supported header fields within the SUBSCRIBE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate  | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 8    | WWW-Authenticate  | [26] 20.44 | m          | m              | [26] 20.44 | m          | m              |
| c1:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480 (Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.140: Supported header fields within the SUBSCRIBE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | o              |

**Table A.141: Void**

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.142: Supported header fields within the SUBSCRIBE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate  | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 6    | WWW-Authenticate  | [26] 20.44 | o          | o              | [26] 20.44 | o          | o              |
| c1:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.143: Supported header fields within the SUBSCRIBE response**

| Item | Header field                                     | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Accept   | [26] 20.1  | o.1        | o.1            | [26] 20.1  | m          | m              |
| 2    | Accept-Encoding                                  | [26] 20.2  | o.1        | o.1            | [26] 20.2  | m          | m              |
| 3    | Accept-Language                                  | [26] 20.3  | o.1        | o.1            | [26] 20.3  | m          | m              |
| 6    | Server   | [26] 20.35 | o          | o              | [26] 20.35 | o          | o              |
| o.1  | At least one of these capabilities is supported. |            |            |                |            |            |                |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.143A: Supported header fields within the SUBSCRIBE response**

| Item | Header field  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority  | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.4/70A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.144: Supported header fields within the SUBSCRIBE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | m          | m              |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.144A: Supported header fields within the SUBSCRIBE response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | x          | x              | [48] 2    | c1         | c1             |
| c1:  | IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/29 - - Additional for 423 (Interval Too Brief) response

**Table A.145: Supported header fields within the SUBSCRIBE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Min-Expires  | [26] 20.23 | m          | m              | [26] 20.23 | m          | m              |



**Table A.146: Void**

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/29H - - Additional for 470 (Consent Needed) response

**Table A.146A: Supported header fields within the SUBSCRIBE response**

| Item | Header field       | Sending        |            |                | Receiving      |            |                |
|------|--------------------|----------------|------------|----------------|----------------|------------|----------------|
|      |                    | Ref.           | RFC status | Profile status | Ref.           | RFC status | Profile status |
| 1    | Permission-Missing | [125]<br>5.9.3 | m          | m              | [125]<br>5.9.3 | m          | m              |

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/39 - - Additional for 489 (Bad Event) response

**Table A.147: Supported header fields within the SUBSCRIBE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Allow-Events | [28] 7.2.2 | m          | m              | [28] 7.2.2 | m          | m              |

**Table A.148: Void**

Prerequisite A.5/21 - - SUBSCRIBE response

**Table A.149: Supported message bodies within the SUBSCRIBE response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

#### A.2.1.4.14 UPDATE method

Prerequisite A.5/22 - - UPDATE request

**Table A.150: Supported header fields within the UPDATE request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | o          | o              | [26] 20.1            | m          | m              |
| 1A   | Accept-Contact                | [56B] 9.2            | c20        | c20            | [56B] 9.2            | c24        | c24            |
| 2    | Accept-Encoding               | [26] 20.2            | o          | o              | [26] 20.2            | m          | m              |
| 3    | Accept-Language               | [26] 20.3            | o          | o              | [26] 20.3            | m          | m              |
| 4    | Allow                         | [26] 20.5            | o          | o              | [26] 20.5            | m          | m              |
| 5    | Allow-Events                  | [28] 7.2.2           | c2         | c2             | [28] 7.2.2           | c3         | c3             |
| 6    | Authorization                 | [26] 20.7            | c4         | c4             | [26] 20.7            | c4         | c4             |
| 7    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 8    | Call-Info                     | [26] 20.9            | o          | o              | [26] 20.9            | o          | o              |
| 9    | Contact                       | [26] 20.10           | m          | m              | [26] 20.10           | m          | m              |
| 10   | Content-Disposition           | [26] 20.11           | o          | o              | [26] 20.11           | m          | m              |
| 11   | Content-Encoding              | [26] 20.12           | o          | o              | [26] 20.12           | m          | m              |
| 12   | Content-Language              | [26] 20.13           | o          | o              | [26] 20.13           | m          | m              |
| 13   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 14   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | m          | m              |
| 15   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 16   | Date                          | [26] 20.17           | c5         | c5             | [26] 20.17           | m          | m              |
| 16A  | Feature-Caps                  | [190]                | c37        | c37            | [190]                | c36        | c36            |
| 17   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 17A  | Geolocation                   | [89] 4.1             | c25        | c25            | [89] 4.1             | c25        | c25            |
| 17B  | Geolocation-Routing           | [89] 4.2             | c25        | c25            | [89] 4.2             | c25        | c25            |
| 17C  | Max-Breadth                   | [117] 5.8            | n/a        | c29            | [117] 5.8            | c30        | c30            |
| 18   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | n/a        | c31            |
| 19   | MIME-Version                  | [26] 20.24           | o          | o              | [26] 20.24           | m          | m              |
| 19A  | Min-SE                        | [58] 5               | c21        | c21            | [58] 5               | c21        | c21            |
| 20   | Organization                  | [26] 20.25           | o          | o              | [26] 20.25           | o          | o              |
| 20A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c11        | c12            | [52] 4.4,<br>[234] 2 | c11        | c13            |
| 20B  | P-Charging-Function-Addresses | [52] 4.5             | c16        | c17            | [52] 4.5             | c16        | c17            |
| 20C  | P-Charging-Vector             | [52] 4.6             | c14        | c15            | [52] 4.6             | c14        | c15            |
| 20E  | P-Early-Media                 | [109] 8              | c26        | c26            | [109] 8              | c26        | c26            |
| 20F  | Privacy                       | [33] 4.2             | c6         | n/a            | [33] 4.2             | c6         | n/a            |
| 21   | Proxy-Authorization           | [26] 20.28           | c10        | c10            | [26] 20.28           | n/a        | n/a            |
| 22   | Proxy-Require                 | [26] 20.29           | o          | n/a            | [26] 20.29           | n/a        | n/a            |
| 22A  | Reason                        | [34A] 2              | c8         | c8             | [34A] 2              | c8         | c8             |
| 23   | Record-Route                  | [26] 20.30           | n/a        | c31            | [26] 20.30           | n/a        | c31            |
| 23A  | Recv-Info                     | [25] 5.2.3           | c34        | c34            | [25] 5.2.3           | c34        | c34            |
| 23B  | Referred-By                   | [59] 3               | c22        | c22            | [59] 3               | c23        | c23            |
| 23C  | Reject-Contact                | [56B] 9.2            | c20        | c20            | [56B] 9.2            | c24        | c24            |
| 23D  | Request-Disposition           | [56B] 9.1            | c20        | c20            | [56B] 9.1            | c24        | c24            |
| 24   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | m          | m              |
| 24A  | Resource-Priority             | [116] 3.1            | c33        | c33            | [116] 3.1            | c33        | c33            |
| 25   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | n/a        | c31            |
| 25A  | Security-Client               | [48] 2.3.1           | c18        | c18            | [48] 2.3.1           | n/a        | n/a            |
| 25B  | Security-Verify               | [48] 2.3.1           | c19        | c19            | [48] 2.3.1           | n/a        | n/a            |
| 25C  | Session-Expires               | [58] 4               | c21        | c21            | [58] 4               | c21        | c21            |
| 25D  | Session-ID                    | [162]                | o          | c35            | [162]                | o          | c35            |
| 26   | Supported                     | [26] 20.37           | o          | o              | [26] 20.37           | m          | m              |
| 27   | Timestamp                     | [26] 20.38           | c9         | c9             | [26] 20.38           | m          | m              |
| 28   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 29   | User-Agent                    | [26] 20.41           | o          | o              | [26] 20.41           | o          | o              |
| 30   | Via                           | [26] 20.42           | m          | m              | [26] 20.42           | m          | m              |

|       |   |
|-------|---|
| c2:   | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.  |
| c3:   | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.  |
| c4:   | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.  |
| c5:   | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.  |
| c6:   | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c8:   | IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c9:   | IF A.4/6 THEN o ELSE n/a - - timestamping of requests.  |
| c10:  | IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.  |
| c11:  | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.   |
| c12:  | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.  |
| c13:  | IF A.4/34 AND (A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA, AS acting as third-party call controller or EATF.  |
| c14:  | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.   |
| c15:  | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c16:  | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c17:  | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c18:  | IF A.4/37 OR A.4/37A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note).   |
| c19:  | IF A.4/37 OR A.4/37A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |
| c20:  | IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.   |
| c21:  | IF A.4/42 THEN m ELSE n/a - - the SIP session timer.  |
| c22:  | IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c23:  | IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.  |
| c24:  | IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c25:  | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.  |
| c26:  | IF A.4/66 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.  |
| c29:  | IF A.4/71 AND (A.3/9B OR A.3/9C OR A.3/13B OR A.3/13C) THEN m ELSE IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - addressing an amplification vulnerability in session initiation protocol forking proxies, IBCF (IMS-ALG), IBCF (Screening of SIP signalling), ISC gateway function (IMS-ALG), ISC gateway function (Screening of SIP signalling), UE, UE performing the functions of an external attached network. |
| c30:  | IF A.4/71 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |
| c31:  | IF A.3/1 AND NOT A.3C/1 THEN n/a ELSE o - - UE, UE performing the functions of an external attached network.  |
| c33:  | IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.   |
| c34:  | IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.  |
| c35:  | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.  |
| c36:  | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.   |
| c37:  | IF A.4/100 AND A.3/1 AND NOT A.3C/1 THEN n/a ELSE IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy, UE, UE performing the functions of an external attached network.  |
| NOTE: | Support of this header field in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header field in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].   |

Prerequisite A.5/22 - - UPDATE request

**Table A.151: Supported message bodies within the UPDATE request**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/1 - - Additional for 100 (Trying) response

**Table A.151A: Supported header fields within the UPDATE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID  | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length   | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq   | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date   | [26] 20.17 | c1         | c1             | [26] 20.17 | m          | m              |
| 5    | From   | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To   | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via  | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses. |            |            |                |            |            |                |

Prerequisite A.5/23 - - UPDATE response for all remaining status-codes

**Table A.152: Supported header fields within the UPDATE response**

| Item  | Header field   | Sending                          |            |                | Receiving                        |            |                |
|-------|--|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|       |  | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A    | Allow  | [26] 20.5                        | c11        | c11            | [26] 20.5                        | m          | m              |
| 1     | Call-ID  | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 1A    | Call-Info  | [26] 20.9                        | o          | o              | [26] 20.9                        | o          | o              |
| 1B    | Contact  | [26] 20.10                       | o          | o              | [26] 20.10                       | o          | o              |
| 2     | Content-Disposition  | [26] 20.11                       | o          | o              | [26] 20.11                       | m          | m              |
| 3     | Content-Encoding   | [26] 20.12                       | o          | o              | [26] 20.12                       | m          | m              |
| 4     | Content-Language   | [26] 20.13                       | o          | o              | [26] 20.13                       | m          | m              |
| 5     | Content-Length   | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6     | Content-Type   | [26] 20.15                       | m          | m              | [26] 20.15                       | m          | m              |
| 7     | CSeq   | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8     | Date   | [26] 20.17                       | c1         | c1             | [26] 20.17                       | m          | m              |
| 9     | From   | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A    | Geolocation-Error  | [89] 4.3                         | c13        | c13            | [89] 4.3                         | c13        | c13            |
| 10    | MIME-Version   | [26] 20.24                       | o          | o              | [26] 20.24                       | m          | m              |
| 10A   | Organization   | [26] 20.25                       | o          | o              | [26] 20.25                       | o          | o              |
| 10B   | P-Access-Network-Info  | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c4         | c5             | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c4         | c6             |
| 10C   | P-Charging-Function-Addresses  | [52] 4.5,<br>[52A] 4             | c9         | c10            | [52] 4.5,<br>[52A] 4             | c9         | c10            |
| 10D   | P-Charging-Vector  | [52] 4.6,<br>[52A] 4             | c7         | c8             | [52] 4.6,<br>[52A] 4             | c7         | c8             |
| 10F   | Privacy  | [33] 4.2                         | c3         | n/a            | [33] 4.2                         | c3         | n/a            |
| 10G   | Recv-Info  | [25] 5.2.3                       | c16        | c16            | [25] 5.2.3                       | c16        | c16            |
| 10H   | Require  | [26] 20.31                       | m          | m              | [26] 20.31                       | m          | m              |
| 10I   | Server   | [26] 20.35                       | o          | o              | [26] 20.35                       | o          | o              |
| 10J   | Session-ID   | [162]                            | o          | c17            | [162]                            | o          | c17            |
| 11    | Timestamp  | [26] 20.38                       | c12        | c12            | [26] 20.38                       | c2         | c2             |
| 12    | To   | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 12A   | User-Agent   | [26] 20.41                       | o          | o              | [26] 20.41                       | o          | o              |
| 13    | Via  | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 14    | Warning  | [26] 20.43                       | o (note)   | o              | [26] 20.43                       | o          | o              |
| c1:   | IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c2:   | IF A.4/6 THEN m ELSE n/a - - timestamping of requests.   |                                  |            |                |                                  |            |                |
| c3:   | IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |                                  |            |                |                                  |            |                |
| c4:   | IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.  |                                  |            |                |                                  |            |                |
| c5:   | IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.   |                                  |            |                |                                  |            |                |
| c6:   | IF A.4/34 AND (A.3/7A OR A.3/7D OR A3A/84) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA, AS acting as third-party call controller or EATF. |                                  |            |                |                                  |            |                |
| c7:   | IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c8:   | IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c9:   | IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c10:  | IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.  |                                  |            |                |                                  |            |                |
| c11:  | IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed)   |                                  |            |                |                                  |            |                |
| c12:  | IF A.4/6 THEN o ELSE n/a - - timestamping of requests.   |                                  |            |                |                                  |            |                |
| c13:  | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.   |                                  |            |                |                                  |            |                |
| c16:  | IF A.4/13 THEN m ELSE IF A.4/13A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage.   |                                  |            |                |                                  |            |                |
| c17:  | IF A.4/91 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |
| NOTE: | For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header field as SHOULD rather than OPTIONAL.  |                                  |            |                |                                  |            |                |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/102 - - Additional for 2xx response

**Table A.153: Supported header fields within the UPDATE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Accept   | [26] 20.1  | o          | o              | [26] 20.1  | m          | m              |
| 0B   | Accept-Encoding  | [26] 20.2  | o          | o              | [26] 20.2  | m          | m              |
| 0C   | Accept-Language  | [26] 20.3  | o          | o              | [26] 20.3  | m          | m              |
| 0D   | Accept-Resource-Priority   | [116] 3.2  | c14        | c14            | [116] 3.2  | c14        | c14            |
| 1    | Allow-Events   | [28] 7.2.2 | c4         | c4             | [28] 7.2.2 | c5         | c5             |
| 2    | Authentication-Info  | [26] 20.6  | c1         | c1             | [26] 20.6  | c2         | c2             |
| 3    | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | m          | m              |
| 3A   | Feature-Caps   | [190]      | c16        | c16            | [190]      | c16        | c16            |
| 3B   | P-Early-Media  | [109] 8    | c6         | c6             | [109] 8    | c6         | c6             |
| 4    | Session-Expires  | [58]       | c3         | c3             | [58]       | c3         | c3             |
| 6    | Supported  | [26] 20.37 | m          | m              | [26] 20.37 | m          | m              |
| c1:  | IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c2:  | IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.   |            |            |                |            |            |                |
| c3:  | IF A.4/42 THEN m ELSE n/a - - the SIP session timer  |            |            |                |            |            |                |
| c4:  | IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.                                     |            |            |                |            |            |                |
| c5:  | IF A.4/23 THEN m ELSE n/a - - acting as the subscriber to event information.                                   |            |            |                |            |            |                |
| c6:  | IF A.4/66 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media. |            |            |                |            |            |                |
| c14: | IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.            |            |            |                |            |            |                |
| c16: | IF A.4/100 THEN m ELSE n/a - - indication of features supported by proxy.                                      |            |            |                |            |            |                |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

**Table A.153A: Supported header fields within the UPDATE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | o          | o              | [26] 20.18 | o          | o              |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx, 485 (Ambiguous) response

**Table A.154: Supported header fields within the UPDATE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Contact      | [26] 20.10 | o          | o              | [26] 20.10 | o          | o              |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/14 - - Additional for 401 (Unauthorized) response

**Table A.154A: Supported header fields within the UPDATE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Proxy-Authenticate  | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 6    | WWW-Authenticate  | [26] 20.44 | m          | m              | [26] 20.44 | m          | m              |
| c1:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.155: Supported header fields within the UPDATE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Retry-After  | [26] 20.33 | o          | o              | [26] 20.33 | o          | o              |

**Table A.156: Void**

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.157: Supported header fields within the UPDATE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Proxy-Authenticate  | [26] 20.27 | c1         | c1             | [26] 20.27 | c1         | c1             |
| 8    | WWW-Authenticate  | [26] 20.44 | o          | o              | [26] 20.44 | o          | o              |
| c1:  | IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA. |            |            |                |            |            |                |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.158: Supported header fields within the UPDATE response**

| Item | Header field                                     | Sending   |            |                | Receiving |            |                |
|------|--|-----------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept   | [26] 20.1 | o.1        | o.1            | [26] 20.1 | m          | m              |
| 2    | Accept-Encoding                                  | [26] 20.2 | o.1        | o.1            | [26] 20.2 | m          | m              |
| 3    | Accept-Language                                  | [26] 20.3 | o.1        | o.1            | [26] 20.3 | m          | m              |
| o.1  | At least one of these capabilities is supported. |           |            |                |           |            |                |



Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.158A: Supported header fields within the UPDATE response**

| Item  | Header field             | Sending   |            |                | Receiving |            |                |
|---|--------------------------|-----------|------------|----------------|-----------|------------|----------------|
|   |                          | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1   | Accept-Resource-Priority | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1: IF A.4/70 THEN m ELSE n/a - - communications resource priority for the session initiation protocol. |                          |           |            |                |           |            |                |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/27 - - Additional for 420 (Bad Extension) response

**Table A.159: Supported header fields within the UPDATE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 7    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | m          | m              |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/28 OR A.6/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.159A: Supported header fields within the UPDATE response**

| Item  | Header field    | Sending |            |                | Receiving |            |                |
|---|-----------------|---------|------------|----------------|-----------|------------|----------------|
|   |                 | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3   | Security-Server | [48] 2  | x          | x              | [48] 2    | c1         | c1             |
| c1: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |                 |         |            |                |           |            |                |

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/28A - - Additional for 422 (Session Interval Too Small) response

**Table A.159B: Supported header fields within the UPDATE response**

| Item   | Header field | Sending |            |                | Receiving |            |                |
|--|--------------|---------|------------|----------------|-----------|------------|----------------|
|  |              | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1  | Min-SE       | [58] 5  | c1         | c1             | [58] 5    | c1         | c1             |
| c1: IF A.4/42 THEN m ELSE n/a - - the SIP session timer. |              |         |            |                |           |            |                |

**Table A.160: Void**

Prerequisite A.5/23 - - UPDATE response

**Table A.161: Supported message bodies within the UPDATE response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

## A.2.2 Proxy role

### A.2.2.1 Introduction

This subclause contains the ICS proforma tables related to the proxy role. They need to be completed only for proxy implementations.

Prerequisite: A.2/2 - - proxy role

## A.2.2.2 Major capabilities

**Table A.162: Major capabilities**

| Item | Does the implementation support   | Reference           | RFC status | Profile status |
|------|---|---------------------|------------|----------------|
|      | <b>Capabilities within main protocol</b>  |                     |            |                |
| 3    | initiate session release?   | [26] 16             | x          | c27            |
| 4    | stateless proxy behaviour?  | [26] 16.11          | o.1        | c29            |
| 5    | stateful proxy behaviour?   | [26] 16.2           | o.1        | c28            |
| 6    | forking of initial requests?  | [26] 16.1           | c1         | c31            |
| 7    | support of indication of TLS connections in the Record-Route header on the upstream side?                                       | [26] 16.7           | o          | n/a            |
| 8    | support of indication TLS connections in the Record-Route header on the downstream side?  | [26] 16.7           | o          | n/a            |
| 8A   | authentication between UA and proxy?  | [26] 20.28, 22.3    | o          | c85            |
| 9    | insertion of date in requests and responses?  | [26] 20.17          | o          | o              |
| 10   | suppression or modification of alerting information data?   | [26] 20.4           | o          | o              |
| 11   | reading the contents of the Require header before proxying the request or response?   | [26] 20.32          | o          | o              |
| 12   | adding or modifying the contents of the Require header before proxying the REGISTER request or response                         | [26] 20.32          | o          | m              |
| 13   | adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER? | [26] 20.32          | o          | o              |
| 14   | being able to insert itself in the subsequent transactions in a dialog (record-routing)?  | [26] 16.6           | o          | c2             |
| 15   | the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routing?         | [26] 16.7           | c3         | c3             |
| 16   | reading the contents of the Supported header before proxying the response?  | [26] 20.37          | o          | o              |
| 17   | reading the contents of the Unsupported header before proxying the 420 response to a REGISTER?                                  | [26] 20.40          | o          | m              |
| 18   | reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER?                | [26] 20.40          | o          | o              |
| 19   | the inclusion of the Error-Info header in 3xx - 6xx responses?  | [26] 20.18          | o          | o              |
| 19A  | reading the contents of the Organization header before proxying the request or response?  | [26] 20.25          | o          | o              |
| 19B  | adding or concatenating the Organization header before proxying the request or response?  | [26] 20.25          | o          | o              |
| 19C  | reading the contents of the Call-Info header before proxying the request or response?   | [26] 20.9           | o          | o              |
| 19D  | adding or concatenating the Call-Info header before proxying the request or response?   | [26] 20.9           | o          | o              |
| 19E  | delete Contact headers from 3xx responses prior to relaying the response?   | [26] 20             | o          | o              |
| 19F  | proxy reading the contents of a body or including a body in a request or response?  | [26]                | o          | c88            |
| 19G  | proxy modifying the content of a body   | 3GPP TS 24.237 [8M] | n/a        | C103           |
|      | <b>Extensions</b>   |                     |            |                |

|     |  |                   |     |     |
|-----|--|-------------------|-----|-----|
| 20  | SIP INFO method and package framework?   | [25]              | o   | o   |
| 20A | legacy INFO usage?   | [25] 2, 3         | o   | o   |
| 21  | reliability of provisional responses in SIP?   | [27]              | o   | i   |
| 22  | the REFER method?  | [36]              | o   | o   |
| 23  | integration of resource management and SIP?  | [30] [64]         | o   | i   |
| 24  | the SIP UPDATE method?   | [29]              | c4  | i   |
| 26  | SIP extensions for media authorization?  | [31]              | o   | c7  |
| 27  | SIP specific event notification  | [28]              | o   | i   |
| 28  | the use of NOTIFY to establish a dialog  | [28] 4.2          | o   | n/a |
| 29  | Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts   | [35]              | o   | c6  |
| 30  | private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks  | [34]              | o   | m   |
| 30A | act as first entity within the trust domain for asserted identity?   | [34]              | c5  | c9  |
| 30B | act as entity within trust network that can route outside the trust network?   | [34]              | c5  | c9  |
| 30C | act as entity passing on identity transparently independent of trust domain?   | [34]              | c5  | c96 |
| 31  | a privacy mechanism for the Session Initiation Protocol (SIP)  | [33]              | o   | m   |
| 31A | request of privacy by the inclusion of a Privacy header  | [33]              | n/a | n/a |
| 31B | application of privacy based on the received Privacy header  | [33]              | c10 | c12 |
| 31C | passing on of the Privacy header transparently   | [33]              | c10 | c13 |
| 31D | application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the assistance of intermediaries are obscured? | [33] 5.1          | x   | x   |
| 31E | application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs?   | [33] 5.2          | n/a | n/a |
| 31F | application of the privacy option "user" such that user level privacy functions are provided by the network?   | [33] 5.3          | n/a | n/a |
| 31G | application of the privacy option "id" such that privacy of the network asserted identity is provided by the network?  | [34] 7            | c11 | c12 |
| 31H | application of the privacy option "history" such that privacy of the History-Info header is provided by the network?   | [66] 7.2          | c34 | c34 |
| 32  | Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration   | [38]              | o   | c30 |
| 33  | a messaging mechanism for the Session Initiation Protocol (SIP)  | [50]              | o   | m   |
| 34  | Compressing the Session Initiation Protocol  | [55]              | o   | c7  |
| 35  | private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)?  | [52]              | o   | m   |
| 36  | the P-Associated-URI header extension?   | [52] 4.1, [52A] 4 | c14 | c15 |

|     |  |                            |     |     |
|-----|--|----------------------------|-----|-----|
| 37  | the P-Called-Party-ID header extension?  | [52] 4.2, [52A] 4          | c14 | c16 |
| 38  | the P-Visited-Network-ID header extension?   | [52] 4.3, [52A] 4          | c14 | c17 |
| 39  | reading, or deleting the P-Visited-Network-ID header before proxying the request or response?                          | [52] 4.3                   | c18 | n/a |
| 41  | the P-Access-Network-Info header extension?  | [52] 4.4, [52A] 4, [234] 2 | c14 | c19 |
| 42  | act as first entity within the trust domain for access network information?  | [52] 4.4                   | c20 | c21 |
| 43  | act as subsequent entity within trust network for access network information that can route outside the trust network? | [52] 4.4                   | c20 | c22 |
| 44  | the P-Charging-Function-Addresses header extension?  | [52] 4.5, [52A] 4          | c14 | m   |
| 44A | adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response?          | [52] 4.6                   | c25 | c26 |
| 45  | the P-Charging-Vector header extension?  | [52] 4.6, [52A] 4          | c14 | m   |
| 46  | adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response?           | [52] 4.6                   | c23 | c24 |
| 47  | security mechanism agreement for the session initiation protocol?  | [48]                       | o   | c7  |
| 47A | mediasec header field parameter for marking security mechanisms related to media?                                      | Subclause 7.2A.7           | n/a | c99 |
| 48  | the Reason header field for the session initiation protocol  | [34A]                      | o   | c78 |
| 48A | carrying Q.850 codes in reason header fields in SIP (Session Initiation Protocol) responses?                           | [130]                      | o   | o   |
| 49  | an extension to the session initiation protocol for symmetric response routing   | [56A]                      | o   | m   |
| 50  | caller preferences for the session initiation protocol?  | [56B]                      | c33 | c33 |
| 50A | the proxy-directive within caller-preferences?   | [56B] 9.1                  | o.4 | o.4 |
| 50B | the cancel-directive within caller-preferences?  | [56B] 9.1                  | o.4 | o.4 |
| 50C | the fork-directive within caller-preferences?  | [56B] 9.1                  | o.4 | c32 |
| 50D | the recurse-directive within caller-preferences?   | [56B] 9.1                  | o.4 | o.4 |
| 50E | the parallel-directive within caller-preferences?  | [56B] 9.1                  | o.4 | c32 |
| 50F | the queue-directive within caller-preferences?   | [56B] 9.1                  | o.4 | o.4 |
| 51  | an event state publication extension to the session initiation protocol?   | [70]                       | o   | m   |
| 52  | SIP session timer?   | [58]                       | o   | o   |
| 53  | the SIP Referred-By mechanism?   | [59]                       | o   | o   |
| 54  | the Session Initiation Protocol (SIP) "Replaces" header?   | [60]                       | o   | o   |
| 55  | the Session Initiation Protocol (SIP) "Join" header?   | [61]                       | o   | o   |
| 56  | the callee capabilities?   | [62]                       | o   | o   |
| 57  | an extension to the session initiation protocol for request history information?                                       | [66]                       | o   | o   |
| 58  | Rejecting anonymous requests in the session initiation protocol?   | [67]                       | o   | o   |

|     |   |           |     |           |
|-----|---|-----------|-----|-----------|
| 59  | session initiation protocol URIs for applications such as voicemail and interactive voice response                              | [68]      | o   | o         |
| 60  | the P-User-Database private header extension?   | [82]      | o   | c95       |
| 61  | Session initiation protocol's non-INVITE transactions?  | [84]      | m   | m         |
| 62  | a uniform resource name for services  | [69]      | n/a | c35       |
| 63  | obtaining and using GRUUs in the Session Initiation Protocol (SIP)  | [93]      | o   | c36       |
| 65  | the Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)?                       | [96]      | o   | o (note2) |
| 66  | the SIP P-Profile-Key private header extension?   | [97]      | o   | c41       |
| 66A | making the first query to the database in order to populate the P-Profile-Key header?   | [97]      | c38 | c39       |
| 66B | using the information in the P-Profile-Key header?  | [97]      | c38 | c40       |
| 67  | managing client initiated connections in SIP?   | [92] 11   | o   | c42       |
| 68  | indicating support for interactive connectivity establishment in SIP?   | [102]     | o   | o         |
| 69  | multiple-recipient MESSAGE requests in the session initiation protocol  | [104]     | n/a | n/a       |
| 70  | SIP location conveyance?  | [89]      | o   | c94       |
| 70A | addition or modification of location in a SIP method?   | [89]      | c44 | c45       |
| 70B | passes on locations in SIP method without modification?   | [89]      | c44 | c46       |
| 71  | referring to multiple resources in the session initiation protocol?   | [105]     | n/a | n/a       |
| 72  | conference establishment using request-contained lists in the session initiation protocol?                                      | [106]     | n/a | n/a       |
| 73  | subscriptions to request-contained resource lists in the session initiation protocol?   | [107]     | n/a | n/a       |
| 74  | dialstring parameter for the session initiation protocol uniform resource identifier?   | [103]     | o   | n/a       |
| 75  | the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular? | [111]     | o   | c60       |
| 76  | the SIP P-Early-Media private header extension for authorization of early media?  | [109] 8   | o   | c51       |
| 77  | number portability parameters for the 'tel' URI?  | [112]     | o   | c47       |
| 77A | assert or process carrier indication?   | [112]     | o   | c48       |
| 77B | local number portability?   | [112]     | o   | c50       |
| 79  | extending the session initiation protocol Reason header for preemption events   | [115]     | c79 | c79       |
| 80  | communications resource priority for the session initiation protocol?   | [116]     | o   | c80       |
| 80A | inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol?                | [116] 4.2 | c82 | c82       |
| 80B | inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol?         | [116] 4.2 | c82 | c82       |

|     |   |                   |      |      |
|-----|---|-------------------|------|------|
| 81  | addressing an amplification vulnerability in session initiation protocol forking proxies?                       | [117]             | c52  | c52  |
| 82  | the remote application identification of applying signalling compression to SIP                                 | [79] 9.1          | o    | c7   |
| 83  | a session initiation protocol media feature tag for MIME application subtypes?                                  | [120]             | o    | c53  |
| 84  | SIP extension for the identification of services?   | [121]             | o    | c54  |
| 84A | act as authentication entity within the trust domain for asserted service?                                      | [121]             | c55  | c56  |
| 85  | a framework for consent-based communications in SIP?  | [125]             | o    | m    |
| 86  | a mechanism for transporting user-to-user call control information in SIP?                                      | [126]             | o    | c84  |
| 87  | the SIP P-Private-Network-Indication private-header (P-Header)?   | [134]             | o    | o    |
| 88  | the SIP P-Served-User private header in the 3GG IM CN subsystem?  | [133] 6           | o    | o    |
| 89  | the SIP P-Served-User header extension for Originating CDIV session case?                                       | [239] 4           | c126 | c126 |
| 91  | the 199 (Early Dialog Terminated) response code   | [142]             | o    | c90  |
| 92  | message body handling in SIP?   | [150]             | o    | c89  |
| 93  | indication of support for keep-alive?   | [143]             | o    | c51  |
| 94  | SIP Interface to VoiceXML Media Services?   | [145]             | o    | c91  |
| 95  | common presence and instant messaging (CPIM): message format?   | [151]             | o    | o    |
| 96  | instant message disposition notification?   | [157]             | o    | o    |
| 97  | requesting answering modes for SIP?   | [158]             | o    | o    |
| 97A | adding, deleting or reading the Answer-Mode header or Priv-Answer-Mode before proxying the request or response? | [158]             | o    | c92  |
| 99  | the early session disposition type for SIP?   | [74B]             | i    | i    |
| 100 | delivery of Request-URI Targets to User Agents?   | Subclause 7.2A.16 | o    | c97  |
| 101 | The Session-ID header?  | [162]             | o    | o    |
| 102 | correct transaction handling for 2xx responses to Session Initiation Protocol INVITE requests?                  | [163]             | m    | m    |
| 103 | addressing Record-Route issues in the Session Initiation Protocol (SIP)?  | [164]             | o    | o    |
| 104 | essential correction for IPv6 ABNF and URI comparison in RFC3261?   | [165]             | m    | m    |
| 105 | suppression of session initiation protocol REFER method implicit subscription?                                  | [173]             | o    | c100 |
| 106 | Alert-Info URNs for the Session Initiation Protocol?  | [175]             | o    | o    |
| 107 | multiple registrations?   | Subclause 3.1     | n/a  | c101 |
| 108 | the SIP P-Refused-URI-List private-header?  | [183]             | o    | c102 |
| 109 | request authorization through dialog Identification in the session initiation protocol?                         | [184]             | o    | o    |
| 110 | indication of features supported by proxy?  | [190]             | o    | c104 |
| 111 | registration of bulk number contacts?   | [191]             | o    | c105 |
| 112 | media control channel framework?  | [146]             | n/a  | n/a  |



|      |                                |                  |      |      |
|------|--------------------------------|------------------|------|------|
| 113  | S-CSCF restoration procedures? | Subclause<br>3.1 | n/a  | n/a  |
| 114  | SIP overload control?          | [198]            | o    | o    |
| 114A | feedback control?              | [199]            | c106 | c106 |
| 114B | distribution of load filters?  | [201]            | n/a  | n/a  |

|      |   |
|------|---|
| c1:  | IF A.162/5 THEN o ELSE n/a - - stateful proxy behaviour.  |
| c2:  | IF A.3/2 OR A.3/9A OR A.3/4 OR A.3/13A OR A.3A/88 THEN m ELSE o - - P-CSCF, IBCF (THIG), S-CSCF, ISC gateway function (THIG), ATCF (proxy).   |
| c3:  | IF A.162/7 AND NOT A.162/8 OR (NOT A.162/7 AND A.162/8) THEN m ELSE IF A.162/14 THEN o ELSE n/a - - TLS interworking with non-TLS else proxy insertion.   |
| c4:  | IF A.162/23 THEN m ELSE o - - integration of resource management and SIP.   |
| c5:  | IF A.162/30 THEN o ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c6:  | IF A.3/2 OR A.3/9A OR A.3A/88 THEN m ELSE n/a - - P-CSCF, IBCF (THIG), ATCF (proxy).  |
| c7:  | IF A.3/2 AND (A.3D/1 OR A.3D/4) THEN m ELSE n/a - - P-CSCF and (IMS AKA plus IPsec ESP or SIP digest with TLS).   |
| c9:  | IF (A.3/2 OR A.3/4 OR A.3/9A OR A.3/13A) AND A.162/30 THEN m ELSE IF A.3/7C AND A.162/30 THEN o ELSE n/a - - P-CSCF or S-CSCF or IBCF (THIG) or ISC gateway function (THIG) or AS acting as proxy and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks (NOTE 1). |
| c10: | IF A.162/31 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c11: | IF A.162/31B THEN o ELSE x - - application of privacy based on the received Privacy header.   |
| c12: | IF A.162/31 AND A.3/4 THEN m ELSE IF A.3/11 THEN o ELSE n/a - - S-CSCF, E-CSCF.   |
| c13: | IF A.162/31 AND (A.3/2 OR A.3/3 OR A.3/7C OR A.3/9A OR A.3/13A OR A.3A/88) THEN m ELSE n/a - - P-CSCF, I-CSCF, AS acting as a SIP proxy or IBCF (THIG), ISC gateway function (THIG), ATCF (proxy).  |
| c14: | IF A.162/35 THEN o.3 ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP).   |
| c15: | IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/9A OR A.3/13A) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF or IBCF (THIG) or ISC gateway function (THIG).  |
| c16: | IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/4 OR A.3/9A OR A.3/13A) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF or S-CSCF or IBCF (THIG) or ISC gateway function (THIG).                                   |
| c17: | IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/9A OR A.3/13A) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF or IBCF (THIG) or ISC gateway function (THIG).  |
| c18: | IF A.162/38 THEN o ELSE n/a - - the P-Visited-Network-ID header extension.  |
| c19: | IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/4 OR A.3/7) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF, I-CSCF, S-CSCF, AS acting as a proxy.   |
| c20: | IF A.162/41 THEN o ELSE n/a - - the P-Access-Network-Info header extension.   |
| c21: | IF A.162/41 AND A.3/2 THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF.  |
| c22: | IF A.162/41 AND A.3/4 THEN m ELSE n/a - - the P-Access-Network-Info header extension and S-CSCF.  |
| c23: | IF A.162/45 THEN o ELSE n/a - - the P-Charging-Vector header extension.   |
| c24: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c25: | IF A.162/44 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c26: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c27: | IF A.3/2 OR A.3/4 THEN m ELSE x - - P-CSCF or S-CSCF.   |
| c28: | IF A.3/2 OR A.3/3 OR A.3/4 THEN m ELSE o.8 - - P-CSCF or I-CSCF or S-CSCF.  |
| c29: | IF A.3/2 OR A.3/4 THEN n/a ELSE IF A.3/3 THEN o ELSE o.8 - - P-CSCF or S-CSCF or I-CSCF.  |
| c30: | IF A.3/2 o ELSE i - - P-CSCF.   |
| c31: | IF A.3/4 THEN m ELSE x - - S-CSCF.  |
| c32: | IF A.3/4 THEN m ELSE o.4 - - S-CSCF.  |
| c33: | IF A.162/50A OR A.162/50B OR A.162/50C OR A.162/50D OR A.162/50E OR A.162/50F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol.  |
| c34: | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |

|       |  |
|-------|--|
| c35:  | IF A.3/2 OR A.3/11 THEN m ELSE IF A.3/7C OR A.3/9A OR A.3/13A THEN o ELSE n/a - - P-CSCF, E-CSCF, AS acting as proxy, IBCF (THIG), ISC gateway function (THIG).  |
| c36:  | IF A.3/4 THEN m ELSE n/a - - S-CSCF.   |
| c38:  | IF A.162/66 THEN o ELSE n/a - - the SIP P-Profile-Key private header.  |
| c39:  | IF A.162/66 AND (A.3/3 OR A.3/9A) THEN m ELSE n/a - - the SIP P-Profile-Key private header, I-CSCF or IBCF (THIG).   |
| c40:  | IF A.162/66 AND A.3/4 THEN m ELSE n/a - - the SIP P-Profile-Key private header, S-CSCF.  |
| c41:  | IF A.3/3 OR A.3/4 OR A.3/9A THEN o ELSE n/a - - I-CSCF or S-CSCF or IBCF (THIG).   |
| c42:  | IF A.162/107 THEN m ELSE n/a - - multiple registrations.   |
| c44:  | IF A.162/70 THEN o.5 ELSE n/a - - SIP location conveyance.   |
| c45:  | IF A.3/11 THEN m ELSE IF A.162/70 AND A.3/7C THEN o.6 ELSE n/a - - E-CSCF, SIP location conveyance, AS acting as a SIP proxy.  |
| c46:  | IF A.162/70 AND A.3/2 OR A.3/3 OR A.3/5 OR A.3/10 OR A.3A/88 THEN m ELSE IF A.162/70 AND A.3/7C THEN o.6 ELSE n/a - - SIP location conveyance, P-CSCF, I-CSCF, S-CSCF, BGCF, additional routeing functionality, ATCF (proxy).                                |
| c47:  | IF A.3/3 OR A.3/4 OR A.3/5 OR A.3/7C THEN o ELSE n/a - - I-CSCF, S-CSCF, BGCF, AS acting as a SIP proxy.   |
| c48:  | IF A.162/77 THEN m ELSE n/a - - number portability parameters for the 'tel' URI.   |
| c50:  | IF A.162/77 THEN m ELSE n/a - - number portability parameters for the 'tel' URI.   |
| c51:  | IF A.3/2 THEN m ELSE o - - P-CSCF.   |
| c52:  | IF A.162/6 THEN m ELSE o - - forking of initial requests.  |
| c53:  | IF A.3/4 THEN m ELSE n/a - - S-CSCF.   |
| c54:  | IF A.3/3 OR A.3/4 OR A.3/7 OR A.3/2 OR A.3/9A OR A.3/13A THEN m ELSE n/a - - I-CSCF, S-CSCF, BGCF, P-CSCF, IBCF (THIG), ISC gateway function (THIG).   |
| c55:  | IF A.162/84 THEN o ELSE n/a - - SIP extension for the identification of services.  |
| c56:  | IF A.3/4 AND A.162/84 THEN m ELSE n/a - - S-CSCF and SIP extension for the identification of services.   |
| c60:  | IF A.3/2 OR A.3/3 OR A.3/4 THEN o ELSE n/a - - P=CSCF, I-CSCF, S-CSCF.   |
| c78:  | IF A.162/79 OR A.162/3 THEN m ELSE o - - extending the session initiation protocol Reason header for preemption events, initiate session release.  |
| c79:  | IF A.162/80 THEN o ELSE n/a - - communications resource priority for the session initiation protocol.  |
| c80:  | IF A.3/2 OR A.3/3 OR A.3/4 OR A.3/5 OR A.3/7C OR A.3/9A OR A.3/10 OR A.3/13A THEN o ELSE n/a - - P-CSCF, I-CSCF, S-CSCF, BGCF, AS acting as proxy, IBCF (THIG), additional routeing functionality, ISC gateway function (THIG).                              |
| c82:  | IF A.162/80 THEN o ELSE n/a - - communications resource priority for the session initiation protocol.  |
| c84:  | A.3/2 OR A.3/3 OR A.3/4 OR A.3/5 OR A.3/7C OR A.3/9A OR A.3/10 OR A.3/11 OR A.3/13A THEN o ELSE n/a - - P-CSCF, I-CSCF, S-CSCF, BGCF, AS acting as proxy, IBCF (THIG), additional routeing functionality, E-CSCF, ISC gateway function (THIG).               |
| c85:  | IF A.3/2 OR A.3/3 OR A.3/4 THEN o ELSE x - - P-CSCF, I-CSCF, S-CSCF.   |
| c88:  | IF A.3/2 OR A.3/4 OR A.3/7 OR A.3/7C OR A.3/9C OR A.3/11 OR A.3/13C OR A.3A/88 THEN m ELSE o - - P-CSCF, S-CSCF, AS, AS acting as a SIP proxy, IBCF (Screening of SIP signalling), E-CSCF, ISC gateway function (Screening of SIP signalling), ATCF (proxy). |
| c89:  | IF A.162/19F THEN m ELSE n/a - - proxy reading the contents of a body or including a body in a request or response.  |
| c90:  | IF A.3/4 THEN m ELSE i - - S-CSCF.   |
| c91:  | IF A.3/4 THEN o ELSE n/a - - S-CSCF.   |
| c92:  | IF A.162/92 THEN o ELSE n/a - - requesting answering modes for SIP.  |
| c94:  | IF A.3/11 THEN m ELSE o - - E-CSCF.  |
| c95:  | IF A.3/3 OR A.3/4 OR A.3/7C THEN o ELSE n/a - - I-CSCF, S-CSCF, AS acting as a SIP proxy.  |
| c96:  | IF A.3/2 OR A.3/11 OR A.3A/88 THEN m ELSE n/a - - P-CSCF, E-CSCF, ATCF (proxy).  |
| c97:  | IF A.3/7 THEN o ELSE n/a - - AS.   |
| c99:  | IF A.3/2A AND A.3D/30 THEN m ELSE n/a - - P-CSCF (IMS-ALG) and end-to-access-edge media security using SDES.   |
| c100: | IF A.4/22 THEN o ELSE n/a - - the REFER method.  |
| c101: | IF A.3/2 OR A.3/4 THEN m ELSE n/a - - P-CSCF, S-CSCF.  |

|         |  |
|---------|--|
| c102:   | IF A.3/9B THEN m ELSE IF A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), AS acting as terminating UA, AS acting as originating UA, AS performing 3 <sup>rd</sup> party call control.  |
| c103:   | IF A.3A/88 THEN m ELSE n/a - - ATCF (proxy).   |
| c104:   | IF A.3/2 OR A.3A/50A OR A.3A/83 OR A.3A/88 THEN m ELSE o - - P-CSCF, Multimedia telephony application server, SCC application server, ATCF (proxy).  |
| c105:   | IF A.3/2 OR A.3/3 OR A.3/9 THEN o ELSE n/a - - P-CSCF, I-CSCF, IBCF.   |
| c106:   | IF A.162/114 THEN o.9 ELSE n/a - - SIP overload control.   |
| c126:   | IF A.162/88 THEN o ELSE n/a - - the SIP P-Served-User private header for the 3GPP IM CN subsystem.   |
| o.1:    | It is mandatory to support at least one of these items.  |
| o.2:    | It is mandatory to support at least one of these items.  |
| o.3:    | It is mandatory to support at least one of these items.  |
| o.4:    | At least one of these capabilities is supported.   |
| o.5:    | It is mandatory to support exactly one of these items.   |
| o.6:    | It is mandatory to support exactly one of these items.   |
| o.7:    | It is mandatory to support at least one of these items.  |
| o.8:    | It is mandatory to support at least one of these items.  |
| o.9:    | At least one of these capabilities is supported.   |
| NOTE 1: | An AS acting as a proxy may be outside the trust domain, and therefore not able to support the capability for that reason; in this case it is perfectly reasonable for the header to be passed on transparently, as specified in the PDU parts of the profile. |
| NOTE 2: | Not applicable over Gm reference point (UE – P-CSCF).  |

## A.2.2.3 PDUs

Table A.163: Supported methods

| Item | PDU  | Sending        |            |                | Receiving      |            |                |
|------|--|----------------|------------|----------------|----------------|------------|----------------|
|      |  | Ref.           | RFC status | Profile status | Ref.           | RFC status | Profile status |
| 1    | ACK request  | [26] 13        | m          | m              | [26] 13        | m          | m              |
| 2    | BYE request  | [26] 16        | m          | m              | [26] 16        | m          | m              |
| 3    | BYE response   | [26] 16        | m          | m              | [26] 16        | m          | m              |
| 4    | CANCEL request   | [26] 16.10     | m          | m              | [26] 16.10     | m          | m              |
| 5    | CANCEL response  | [26] 16.10     | m          | m              | [26] 16.10     | m          | m              |
| 6    | INFO request   | [25] 4.2       | c2         | c2             | [25] 4.2       | c2         | c2             |
| 7    | INFO response  | [25] 4.2       | c2         | c2             | [25] 4.2       | c2         | c2             |
| 8    | INVITE request   | [26] 16        | m          | m              | [26] 16        | m          | m              |
| 9    | INVITE response  | [26] 16        | m          | m              | [26] 16        | m          | m              |
| 9A   | MESSAGE request  | [50] 4         | c5         | c5             | [50] 7         | c5         | c5             |
| 9B   | MESSAGE response   | [50] 4         | c5         | c5             | [50] 7         | c5         | c5             |
| 10   | NOTIFY request   | [28] 8.1.2     | c3         | c3             | [28] 8.1.2     | c3         | c3             |
| 11   | NOTIFY response  | [28] 8.1.2     | c3         | c3             | [28] 8.1.2     | c3         | c3             |
| 12   | OPTIONS request  | [26] 16        | m          | m              | [26] 16        | m          | m              |
| 13   | OPTIONS response   | [26] 16        | m          | m              | [26] 16        | m          | m              |
| 14   | PRACK request  | [27] 6         | c6         | c6             | [27] 6         | c6         | c6             |
| 15   | PRACK response   | [27] 6         | c6         | c6             | [27] 6         | c6         | c6             |
| 15A  | PUBLISH request  | [70]<br>11.1.1 | c20        | c20            | [70]<br>11.1.1 | c20        | c20            |
| 15B  | PUBLISH response   | [70]<br>11.1.1 | c20        | c20            | [70]<br>11.1.1 | c20        | c20            |
| 16   | REFER request  | [36] 3         | c1         | c1             | [36] 3         | c1         | c1             |
| 17   | REFER response   | [36] 3         | c1         | c1             | [36] 3         | c1         | c1             |
| 18   | REGISTER request   | [26] 16        | m          | m              | [26] 16        | m          | m              |
| 19   | REGISTER response  | [26] 16        | m          | m              | [26] 16        | m          | m              |
| 20   | SUBSCRIBE request  | [28] 8.1.1     | c3         | c3             | [28] 8.1.1     | c3         | c3             |
| 21   | SUBSCRIBE response   | [28] 8.1.1     | c3         | c3             | [28] 8.1.1     | c3         | c3             |
| 22   | UPDATE request   | [29] 7         | c4         | c4             | [29] 7         | c4         | c4             |
| 23   | UPDATE response  | [29] 7         | c4         | c4             | [29] 7         | c4         | c4             |
| c1:  | IF A.162/22 THEN m ELSE n/a - - the REFER method.  |                |            |                |                |            |                |
| c2:  | IF A.162/20 OR A.162/20A THEN m ELSE n/a - - SIP INFO method and package framework, legacy INFO usage. |                |            |                |                |            |                |
| c3:  | IF A.162/27 THEN m ELSE n/a - - SIP specific event notification.                                       |                |            |                |                |            |                |
| c4:  | IF A.162/24 THEN m ELSE n/a - - the SIP UPDATE method.   |                |            |                |                |            |                |
| c5:  | IF A.162/33 THEN m ELSE n/a - - the SIP MESSAGE method.  |                |            |                |                |            |                |
| c6:  | IF A.162/21 THEN m ELSE n/a - - reliability of provisional responses.                                  |                |            |                |                |            |                |
| c20: | IF A.4/51 THEN m ELSE n/a  |                |            |                |                |            |                |

## A.2.2.4 PDU parameters

### A.2.2.4.1 Status-codes

**Table A.164: Supported-status codes**

| Item | Header                              | Sending         |            |                | Receiving       |            |                |
|------|-------------------------------------|-----------------|------------|----------------|-----------------|------------|----------------|
|      |                                     | Ref.            | RFC status | Profile status | Ref.            | RFC status | Profile status |
| 1    | 100 (Trying)                        | [26]<br>21.1.1  | c1         | c1             | [26]<br>21.1.1  | c2         | c2             |
| 101  | 1xx response                        | [26] 21.1       | p21        | p21            | [26] 21.1       | p21        | p21            |
| 101A | 18x response                        | [26] 21.1       | p21        | p21            | [26] 21.1       | p21        | p21            |
| 2    | 180 (Ringing)                       | [26]<br>21.1.2  | c3         | c3             | [26]<br>21.1.2  | c3         | c3             |
| 3    | 181 (Call Is Being Forwarded)       | [26]<br>21.1.3  | c3         | c3             | [26]<br>21.1.3  | c3         | c3             |
| 4    | 182 (Queued)                        | [26]<br>21.1.4  | c3         | c3             | [26]<br>21.1.4  | c3         | c3             |
| 5    | 183 (Session Progress)              | [26]<br>21.1.5  | c3         | c3             | [26]<br>21.1.5  | c3         | c3             |
| 5A   | 199 (Early Dialog Terminated)       | [142] 11.1      | c32        | c32            | [142] 11.1      | c32        | c32            |
| 102  | 2xx response                        | [26] 21.2       | p22        | p22            | [26] 21.1       | p22        | p22            |
| 6    | 200 (OK)                            | [26]<br>21.2.1  | m          | m              | [26]<br>21.2.1  | i          | m              |
| 7    | 202 (Accepted)                      | [28] 8.3.1      | c4         | c4             | [28] 8.3.1      | c4         | c4             |
| 103  | 3xx response                        | [26] 21.3       | p23        | p23            | [26] 21.1       | p23        | p23            |
| 8    | 300 (Multiple Choices)              | [26]<br>21.3.1  | m          | m              | [26]<br>21.3.1  | i          | i              |
| 9    | 301 (Moved Permanently)             | [26]<br>21.3.2  | m          | m              | [26]<br>21.3.2  | i          | i              |
| 10   | 302 (Moved Temporarily)             | [26]<br>21.3.3  | m          | m              | [26]<br>21.3.3  | i          | i              |
| 11   | 305 (Use Proxy)                     | [26]<br>21.3.4  | m          | m              | [26]<br>21.3.4  | i          | i              |
| 12   | 380 (Alternative Service)           | [26]<br>21.3.5  | m          | m              | [26]<br>21.3.5  | i          | i              |
| 104  | 4xx response                        | [26] 21.4       | p24        | p24            | [26] 21.4       | p24        | p24            |
| 13   | 400 (Bad Request)                   | [26]<br>21.4.1  | m          | m              | [26]<br>21.4.1  | i          | i              |
| 14   | 401 (Unauthorized)                  | [26]<br>21.4.2  | m          | m              | [26]<br>21.4.2  | i          | c10            |
| 15   | 402 (Payment Required)              | [26]<br>21.4.3  | n/a        | n/a            | [26]<br>21.4.3  | n/a        | n/a            |
| 16   | 403 (Forbidden)                     | [26]<br>21.4.4  | m          | m              | [26]<br>21.4.4  | i          | i              |
| 17   | 404 (Not Found)                     | [26]<br>21.4.5  | m          | m              | [26]<br>21.4.5  | i          | i              |
| 18   | 405 (Method Not Allowed)            | [26]<br>21.4.6  | m          | m              | [26]<br>21.4.6  | i          | i              |
| 19   | 406 (Not Acceptable)                | [26]<br>21.4.7  | m          | m              | [26]<br>21.4.7  | i          | i              |
| 20   | 407 (Proxy Authentication Required) | [26]<br>21.4.8  | m          | m              | [26]<br>21.4.8  | i          | i              |
| 21   | 408 (Request Timeout)               | [26]<br>21.4.9  | c3         | c3             | [26]<br>21.4.9  | i          | i              |
| 22   | 410 (Gone)                          | [26]<br>21.4.10 | m          | m              | [26]<br>21.4.10 | i          | i              |
| 22A  | 412 (Conditional Request Failed)    | [70]<br>11.2.1  | c20        | c20            | [70]<br>11.2.1  | c19        | c19            |
| 23   | 413 (Request Entity Too Large)      | [26]<br>21.4.11 | m          | m              | [26]<br>21.4.11 | i          | i              |
| 24   | 414 (Request-URI Too Large)         | [26]<br>21.4.12 | m          | m              | [26]<br>21.4.12 | i          | i              |
| 25   | 415 (Unsupported Media Type)        | [26]<br>21.4.13 | m          | m              | [26]<br>21.4.13 | i          | i              |
| 26   | 416 (Unsupported URI Scheme)        | [26]<br>21.4.14 | m          | m              | [26]<br>21.4.14 | i          | i              |
| 26A  | 417 (Unknown Resource Priority)     | [116]<br>4.6.2  | c25        | c25            | [116]<br>4.6.2  | c25        | c25            |
| 27   | 420 (Bad Extension)                 | [26]<br>21.4.15 | m          | m              | [26]<br>21.4.15 | i          | i              |

| Item | Header                                 | Sending         |            |                | Receiving       |            |                |
|------|--|-----------------|------------|----------------|-----------------|------------|----------------|
|      |  | Ref.            | RFC status | Profile status | Ref.            | RFC status | Profile status |
| 28   | 421 (Extension Required)               | [26]<br>21.4.16 | m          | m              | [26]<br>21.4.16 | i          | i              |
| 28A  | 422 (Session Interval Too Small)       | [58] 6          | c8         | c8             | [58] 6          | c8         | c8             |
| 29   | 423 (Interval Too Brief)               | [26]<br>21.4.17 | c5         | c5             | [26]<br>21.4.17 | c6         | c6             |
| 29A  | 424 (Bad Location Information)         | [89] 4.2        | c23        | c23            | [89] 4.2        | c24        | c24            |
| 29B  | 429 (Provide Referrer Identity)        | [59] 5          | c9         | c9             | [59] 5          | c9         | c9             |
| 29C  | 430 (Flow Failed)                      | [92] 11         | o          | c21            | [92] 11         | m          | c22            |
| 29D  | 433 (Anonymity Disallowed)             | [67] 4          | c14        | c14            | [67] 4          | c14        | c14            |
| 29E  | 439 (First Hop Lacks Outbound Support) | [92] 11         | c28        | c28            | [92] 11         | c29        | c29            |
| 29F  | 440 (Max Breadth Exceeded)             | [117] 5         | c30        | c30            | [117] 5         | c31        | c31            |
| 29G  | 469 (Bad INFO Package)                 | [25] 4.2        | c33        | c33            | [25] 4.2        | c33        | c33            |
| 29H  | 470 (Consent Needed)                   | [125]<br>5.9.2  | c26        | c26            | [125]<br>5.9.2  | c27        | c27            |
| 30   | 480 (Temporarily not available)        | [26]<br>21.4.18 | m          | m              | [26]<br>21.4.18 | i          | i              |
| 31   | 481 (Call /Transaction Does Not Exist) | [26]<br>21.4.19 | m          | m              | [26]<br>21.4.19 | i          | i              |
| 32   | 482 (Loop Detected)                    | [26]<br>21.4.20 | m          | m              | [26]<br>21.4.20 | i          | i              |
| 33   | 483 (Too Many Hops)                    | [26]<br>21.4.21 | m          | m              | [26]<br>21.4.21 | i          | i              |
| 34   | 484 (Address Incomplete)               | [26]<br>21.4.22 | m          | m              | [26]<br>21.4.22 | i          | i              |
| 35   | 485 (Ambiguous)                        | [26]<br>21.4.23 | m          | m              | [26]<br>21.4.23 | i          | i              |
| 36   | 486 (Busy Here)                        | [26]<br>21.4.24 | m          | m              | [26]<br>21.4.24 | i          | i              |
| 37   | 487 (Request Terminated)               | [26]<br>21.4.25 | m          | m              | [26]<br>21.4.25 | i          | i              |
| 38   | 488 (Not Acceptable Here)              | [26]<br>21.4.26 | m          | m              | [26]<br>21.4.26 | i          | i              |
| 39   | 489 (Bad Event)                        | [28] 7.3.2      | c4         | c4             | [28] 7.3.2      | c4         | c4             |
| 40   | 491 (Request Pending)                  | [26]<br>21.4.27 | m          | m              | [26]<br>21.4.27 | i          | i              |
| 41   | 493 (Undecipherable)                   | [26]<br>21.4.28 | m          | m              | [26]<br>21.4.28 | i          | i              |
| 41A  | 494 (Security Agreement Required)      | [48] 2          | c7         | c7             | [48] 2          | n/a        | n/a            |
| 105  | 5xx response                           | [26] 21.5       | p25        | p25            | [26] 21.5       | p25        | p25            |
| 42   | 500 (Internal Server Error)            | [26]<br>21.5.1  | m          | m              | [26]<br>21.5.1  | i          | i              |
| 43   | 501 (Not Implemented)                  | [26]<br>21.5.2  | m          | m              | [26]<br>21.5.2  | i          | i              |
| 44   | 502 (Bad Gateway)                      | [26]<br>21.5.3  | m          | m              | [26]<br>21.5.3  | i          | i              |
| 45   | 503 (Service Unavailable)              | [26]<br>21.5.4  | m          | m              | [26]<br>21.5.4  | i          | i              |
| 46   | 504 (Server Time-out)                  | [26]<br>21.5.5  | m          | m              | [26]<br>21.5.5  | i          | i              |
| 47   | 505 (Version not supported)            | [26]<br>21.5.6  | m          | m              | [26]<br>21.5.6  | i          | i              |
| 48   | 513 (Message Too Large)                | [26]<br>21.5.7  | m          | m              | [26]<br>21.5.7  | i          | i              |
| 49   | 580 (Precondition Failure)             | [30] 8          | m          | m              | [30] 8          | i          | i              |
| 106  | 6xx response                           | [26] 21.6       | p26        | p26            | [26] 21.6       | p26        | p26            |
| 50   | 600 (Busy Everywhere)                  | [26]<br>21.6.1  | m          | m              | [26]<br>21.6.1  | i          | i              |
| 51   | 603 (Decline)                          | [26]<br>21.6.2  | m          | m              | [26]<br>21.6.2  | i          | i              |



| Item | Header  | Sending        |            |                | Receiving      |            |                |
|------|---|----------------|------------|----------------|----------------|------------|----------------|
|      |   | Ref.           | RFC status | Profile status | Ref.           | RFC status | Profile status |
| 52   | 604 (Does Not Exist Anywhere)   | [26]<br>21.6.3 | m          | m              | [26]<br>21.6.3 | i          | i              |
| 53   | 606 (Not Acceptable)  | [26]<br>21.6.4 | m          | m              | [26]<br>21.6.4 | i          | i              |
| c1:  | IF A.163/3 OR A.163/9 OR A.163/9B OR A.163/11 OR A.163/13 OR A.163/15 OR A.163/15B OR A.163/17 OR A.163/19 OR A.163/21 OR A.163/23 AND A.162/5 THEN m ELSE n/a - - BYE response or INVITE response or MESSAGE response or NOTIFY response or OPTIONS response or PRACK response or PUBLISH response or REFER response or REGISTER response or SUBSCRIBE response or UPDATE response, stateful proxy.  |                |            |                |                |            |                |
| c2:  | IF A.163/3 OR A.163/9 OR A.163/9B OR A.163/11 OR A.163/13 OR A.163/15 OR A.163/15B OR A.163/17 OR A.163/19 OR A.163/21 OR A.163/23 THEN (IF A.162/5 THEN m ELSE i) ELSE n/a - - BYE response or INVITE response or MESSAGE response or NOTIFY response or OPTIONS response or PRACK response or PUBLISH response or REFER response or REGISTER response or SUBSCRIBE response or UPDATE response, stateful proxy.   |                |            |                |                |            |                |
| c3:  | IF A.163/9 THEN m ELSE n/a - - INVITE response.   |                |            |                |                |            |                |
| c4:  | IF A.162/27 THEN m ELSE n/a - - SIP specific event notification.  |                |            |                |                |            |                |
| c5:  | IF A.163/19 OR A.163/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response.  |                |            |                |                |            |                |
| c6:  | IF A.163/19 OR A.163/21 THEN i ELSE n/a - - REGISTER response or SUBSCRIBE response.  |                |            |                |                |            |                |
| c7:  | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.   |                |            |                |                |            |                |
| c8:  | IF A.162/52 THEN m ELSE n/a - - the SIP session timer.  |                |            |                |                |            |                |
| c9:  | IF A.162/53 AND A.163/17 THEN m ELSE n/a - - the SIP Referred-By mechanism and REFER response.  |                |            |                |                |            |                |
| c10: | IF A.3/2 THEN m ELSE i - - P-CSCF.  |                |            |                |                |            |                |
| c14: | IF A.162/58 THEN m ELSE n/a - - rejecting anonymous requests in the session initiation protocol.  |                |            |                |                |            |                |
| c19: | IF A.162/51 THEN i ELSE n/a - - an event state publication extension to the session initiation protocol.  |                |            |                |                |            |                |
| c20: | IF A.162/51 THEN m ELSE n/a - - an event state publication extension to the session initiation protocol.  |                |            |                |                |            |                |
| c21: | IF A.4/57 AND A.3/2 THEN o ELSE n/a - - managing client initiated connections in SIP, P-CSCF.   |                |            |                |                |            |                |
| c22: | IF A.4/57 AND A.3/4 THEN m ELSE i - - managing client initiated connections in SIP, S-CSCF.   |                |            |                |                |            |                |
| c23: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |                |            |                |                |            |                |
| c24: | IF A.162/70 THEN i ELSE n/a - - SIP location conveyance.  |                |            |                |                |            |                |
| c25: | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.   |                |            |                |                |            |                |
| c26: | IF A.162/85 THEN m ELSE n/a - - a framework for consent-based communications in SIP.  |                |            |                |                |            |                |
| c27: | IF A.162/85 THEN i ELSE n/a - - a framework for consent-based communications in SIP.  |                |            |                |                |            |                |
| c28: | IF A.162/57 AND THEN m ELSE n/a - - managing client initiated connections in SIP.   |                |            |                |                |            |                |
| c29: | IF A.162/57 AND THEN i ELSE n/a - - managing client initiated connections in SIP.   |                |            |                |                |            |                |
| c30: | IF A.162/81 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |                |            |                |                |            |                |
| c31: | IF A.162/81 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |                |            |                |                |            |                |
| c32: | IF A.162/91 AND A.163/9 THEN m ELSE n/a - - INVITE response and 199 (Early Dialog Terminated) response.   |                |            |                |                |            |                |
| c33: | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |                |            |                |                |            |                |
| p21: | A.164/2 OR A.164/3 OR A.164/4 OR A.164/5 OR A.164/5A - - 1xx response   |                |            |                |                |            |                |
| p22: | A.164/6 OR A.164/7 - - 2xx response   |                |            |                |                |            |                |
| p23: | A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/13 - - 3xx response   |                |            |                |                |            |                |
| p24: | A.164/14 OR A.164/15 OR A.164/16 OR A.164/17 OR A.164/18 OR A.164/19 OR A.164/20 OR A.164/21 OR A.164/22 OR A.164/22A OR A.164/23 OR A.164/24 OR A.164/25 OR A.164/26 OR A.164/26A OR A.164/27 OR A.164/28 OR A.164/28A OR A.164/29 OR A.164/29A OR A.164/29B OR A.164/29C OR A.164/29D OR A.164/29E OR A.164/29F OR A.164/29G OR A.164/29H OR A.164/30 OR A.164/31 OR A.164/32 OR A.164/33 OR A.164/34 OR A.164/35 OR A.164/36 OR A.164/436 OR A.164/38 OR A.164/39 OR A.164/40 OR A.164/41 OR A.164/41A. - - 4xx response |                |            |                |                |            |                |
| p25: | A.164/42 OR A.164/43 OR A.164/44 OR A.164/45 OR A.164/46 OR A.164/47 OR A.164/48 OR A.164/49 - - 5xx response   |                |            |                |                |            |                |
| p26: | A.164/50 OR A.164/51 OR A.164/52 OR A.164/53 - - 6xx response   |                |            |                |                |            |                |

#### A.2.2.4.2 ACK method

Prerequisite A.163/1 - - ACK request

**Table A.165: Supported header fields within the ACK request**

| Item | Header field          | Sending                          |            |                | Receiving                        |            |                |
|------|-----------------------|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |                       | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 1    | Accept-Contact        | [56B] 9.2                        | c10        | c10            | [56B] 9.2                        | c11        | c11            |
| 2    | Allow-Events          | [28] 7.2.2                       | m          | m              | [28] 7.2.2                       | c1         | c1             |
| 3    | Authorization         | [26] 20.7                        | m          | m              | [26] 20.7                        | i          | i              |
| 4    | Call-ID               | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 6    | Content-Disposition   | [26] 20.11                       | m          | m              | [26] 20.11                       | i          | i              |
| 7    | Content-Encoding      | [26] 20.12                       | m          | m              | [26] 20.12                       | i          | i              |
| 8    | Content-Language      | [26] 20.13                       | m          | m              | [26] 20.13                       | i          | i              |
| 9    | Content-Length        | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 10   | Content-Type          | [26] 20.15                       | m          | m              | [26] 20.15                       | i          | c3             |
| 11   | CSeq                  | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 12   | Date                  | [26] 20.17                       | m          | m              | [26] 20.17                       | c2         | c2             |
| 13   | From                  | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 13A  | Max-Breadth           | [117] 5.8                        | c15        | c15            | [117] 5.8                        | c16        | c16            |
| 14   | Max-Forwards          | [26] 20.22                       | m          | m              | [26] 20.22                       | m          | m              |
| 15   | MIME-Version          | [26] 20.24                       | m          | m              | [26] 20.24                       | i          | c3             |
| 15A  | P-Access-Network-Info | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c20        | c20            | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c21        | c21            |
| 15C  | Privacy               | [33] 4.2                         | c6         | c6             | [33] 4.2                         | c7         | c7             |
| 15D  | P-Charging-Vector     | [52] 4.6,<br>[52A] 4             | c22        | c22            | [52] 4.6,<br>[52A] 4             | c23        | c23            |
| 16   | Proxy-Authorization   | [26] 20.28                       | m          | m              | [26] 20.28                       | c4         | c4             |
| 17   | Proxy-Require         | [26] 20.29                       | m          | m              | [26] 20.29                       | m          | m              |
| 17A  | Reason                | [34A] 2                          | c8         | c8             | [34A] 2                          | c9         | c9             |
| 17B  | Recv-Info             | [25] 5.2.3                       | c17        | c17            | [25] 5.2.3                       | c18        | c18            |
| 17C  | Reject-Contact        | [56B] 9.2                        | c10        | c10            | [56B] 9.2                        | c11        | c11            |
| 17D  | Request-Disposition   | [56B] 9.1                        | c10        | c10            | [56B] 9.1                        | c11        | c11            |
| 18   | Require               | [26] 20.32                       | m          | m              | [26] 20.32                       | c5         | c5             |
| 18A  | Resource-Priority     | [116] 3.1                        | c12        | c12            | [116] 3.1                        | c12        | c47            |
| 19   | Route                 | [26] 20.34                       | m          | m              | [26] 20.34                       | m          | m              |
| 19A  | Session-ID            | [162]                            | c19        | c19            | [162]                            | c19        | c19            |
| 20   | Timestamp             | [26] 20.38                       | m          | m              | [26] 20.38                       | i          | i              |
| 21   | To                    | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 22   | User-Agent            | [26] 20.41                       | m          | m              | [26] 20.41                       | i          | i              |
| 23   | Via                   | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |

|       |   |
|-------|---|
| c1:   | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |
| c2:   | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c3:   | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.   |
| c4:   | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.  |
| c5:   | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6:   | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c7:   | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c8:   | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c9:   | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c10:  | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c11:  | IF A.162/50 THEN i ELSE n/a - - caller preferences for the session initiation protocol.   |
| c12:  | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.   |
| c15:  | IF A.162/81 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |
| c16:  | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, forking of initial requests.  |
| c17:  | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |
| c18:  | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |
| c19:  | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |
| c20:  | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c21:  | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c22:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c23:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension   |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.  |

Prerequisite A.163/1 - - ACK request

**Table A.166: Supported message bodies within the ACK request**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

### A.2.2.4.3 BYE method

Prerequisite A.163/2 - - BYE request

**Table A.167: Supported header fields within the BYE request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | m          | m              | [26] 20.1            | i          | i              |
| 1A   | Accept-Contact                | [56B] 9.2            | c22        | c22            | [56B] 9.2            | c23        | c23            |
| 2    | Accept-Encoding               | [26] 20.2            | m          | m              | [26] 20.2            | i          | i              |
| 3    | Accept-Language               | [26] 20.3            | m          | m              | [26] 20.3            | i          | i              |
| 3A   | Allow                         | [26] 20.5            | m          | m              | [26] 20.5            | i          | i              |
| 4    | Allow-Events                  | [28] 7.2.2           | m          | m              | [28] 7.2.2           | c1         | c1             |
| 5    | Authorization                 | [26] 20.7            | m          | m              | [26] 20.7            | i          | i              |
| 6    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 7    | Content-Disposition           | [26] 20.11           | m          | m              | [26] 20.11           | i          | c3             |
| 8    | Content-Encoding              | [26] 20.12           | m          | m              | [26] 20.12           | i          | c3             |
| 9    | Content-Language              | [26] 20.13           | m          | m              | [26] 20.13           | i          | c3             |
| 10   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 11   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | i          | c3             |
| 12   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 13   | Date                          | [26] 20.17           | m          | m              | [26] 20.17           | c2         | c2             |
| 14   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 14A  | Geolocation                   | [89] 4.1             | c26        | c26            | [89] 4.1             | c27        | c27            |
| 14B  | Geolocation-Routing           | [89] 4.1             | c26        | c26            | [89] 4.1             | c27        | c27            |
| 14C  | Max-Breadth                   | [117] 5.8            | c33        | c33            | [117] 5.8            | c34        | c34            |
| 15   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | m          | m              |
| 16   | MIME-Version                  | [26] 20.24           | m          | m              | [26] 20.24           | i          | c3             |
| 16A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c13        | c13            | [52] 4.4,<br>[234] 2 | c14        | c14            |
| 16B  | P-Asserted-Identity           | [34] 9.1             | c9         | c9             | [34] 9.1             | c10        | c10            |
| 16C  | P-Charging-Function-Addresses | [52] 4.5             | c17        | c17            | [52] 4.5             | c18        | c18            |
| 16D  | P-Charging-Vector             | [52] 4.6             | c15        | n/a            | [52] 4.6             | c16        | n/a            |
| 16F  | P-Preferred-Identity          | [34] 9.2             | x          | x              | [34] 9.2             | c8         | n/a            |
| 16G  | Privacy                       | [33] 4.2             | c11        | c11            | [33] 4.2             | c12        | c12            |
| 17   | Proxy-Authorization           | [26] 20.28           | m          | m              | [26] 20.28           | c4         | c4             |
| 18   | Proxy-Require                 | [26] 20.29           | m          | m              | [26] 20.29           | m          | m              |
| 18A  | Reason                        | [34A] 2              | c20        | c20            | [34A] 2              | c21        | c21            |
| 19   | Record-Route                  | [26] 20.30           | m          | m              | [26] 20.30           | c7         | c7             |
| 19A  | Referred-By                   | [59] 3               | c24        | c24            | [59] 3               | c25        | c25            |
| 19B  | Reject-Contact                | [56B] 9.2            | c22        | c22            | [56B] 9.2            | c23        | c23            |
| 19C  | Request-Disposition           | [56B] 9.1            | c22        | c22            | [56B] 9.1            | c23        | c23            |
| 20   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | c5         | c5             |
| 20A  | Resource-Priority             | [116] 3.1            | c28        | c28            | [116] 3.1            | c28        | c28            |
| 21   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | m          | m              |
| 21A  | Security-Client               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c19        | c19            |
| 21B  | Security-Verify               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c19        | c19            |
| 21C  | Session-ID                    | [162]                | c35        | c35            | [162]                | c35        | c35            |
| 22   | Supported                     | [26] 20.37           | m          | m              | [26] 20.37           | c6         | c6             |
| 23   | Timestamp                     | [26] 20.38           | m          | m              | [26] 20.38           | i          | i              |
| 24   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 25   | User-Agent                    | [26] 20.41           | m          | m              | [26] 20.41           | i          | i              |
| 25A  | User-to-User                  | [126] 7              | c29        | c29            | [126] 7              | c30        | c30            |
| 26   | Via                           | [26] 20.42           | m          | m              | [26] 20.42           | m          | m              |

|       |   |
|-------|---|
| c1:   | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |
| c2:   | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c3:   | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.   |
| c4:   | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.  |
| c5:   | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6:   | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.  |
| c7:   | IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.   |
| c8:   | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.   |
| c9:   | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c10:  | IF A.162/30A OR A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |
| c11:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c12:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c13:  | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c14:  | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c15:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c16:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c17:  | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c18:  | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c19:  | IF A.162/47 OR A.162/47A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |
| c20:  | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c21:  | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c22:  | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c23:  | IF A.162/50 THEN i ELSE n/a - - caller preferences for the session initiation protocol.   |
| c24:  | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.  |
| c25:  | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c26:  | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c27:  | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c28:  | IF A.162/80B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.  |
| c29:  | IF A.162/86 THEN m - - transporting user to user information for call centers using SIP.  |
| c30:  | IF A.162/86 THEN i - - transporting user to user information for call centers using SIP.  |
| c33:  | IF A.162/81 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |
| c34:  | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, forking of initial requests.  |
| c35:  | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.  |

Prerequisite A.163/2 - - BYE request

**Table A.168: Supported message bodies within the BYE request**

| Item | Header   | Sending   |            |                | Receiving |            |                |
|------|--|-----------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | XML Schema for PSTN  | [11B]     |            | c1             | [11B]     |            | i              |
| 2    | VoiceXML expr / namelist data  | [145] 4.2 | m          | c2             | [145] 4.2 | m          | c2             |
| 3    | application/vnd.3gpp.ussd  | [8W]      |            | m              | [8W]      |            | i              |
| c1:  | A.3/3 OR A.3/4 OR A.3/5 OR A.3/7C OR A.3/9A OR A.3/10 OR A.3/11 OR A.3/13A THEN m ELSE n/a - - I-CSCF, S-CSCF, BGCF, AS acting as proxy, IBCF (THIG), additional routing functionality, E-CSCF, ISC gateway function (THIG). |           |            |                |           |            |                |
| c2:  | IF A.162/94 THEN m ELSE n/a - - SIP Interface to VoiceXML Media Services.  |           |            |                |           |            |                |

**Table A.169: Void**

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/1 - - Additional for 100 (Trying) response

**Table A.169A: Supported header fields within the BYE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID   | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length  | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq  | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date  | [26] 20.17 | c1         | c1             | [26] 20.17 | c2         | c2             |
| 5    | From  | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To  | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies. |            |            |                |            |            |                |
| c2:  | IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.   |            |            |                |            |            |                |



Prerequisite A.163/3 - - BYE response

**Table A.170: Supported header fields within the BYE response**

| Item | Header field                  | Sending                          |            |                | Receiving                        |            |                |
|------|-------------------------------|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |                               | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow                         | [26] 20.5                        | m          | m              | [26] 20.5                        | i          | i              |
| 1    | Call-ID                       | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 2    | Content-Disposition           | [26] 20.11                       | m          | m              | [26] 20.11                       | i          | c2             |
| 3    | Content-Encoding              | [26] 20.12                       | m          | m              | [26] 20.12                       | i          | c2             |
| 4    | Content-Language              | [26] 20.13                       | m          | m              | [26] 20.13                       | i          | c2             |
| 5    | Content-Length                | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6    | Content-Type                  | [26] 20.15                       | m          | m              | [26] 20.15                       | i          | c2             |
| 7    | CSeq                          | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8    | Date                          | [26] 20.17                       | m          | m              | [26] 20.17                       | c1         | c1             |
| 9    | From                          | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A   | Geolocation-Error             | [89] 4.3                         | c15        | c15            | [89] 4.3                         | c16        | c16            |
| 10   | MIME-Version                  | [26] 20.24                       | m          | m              | [26] 20.24                       | i          | c2             |
| 10A  | P-Access-Network-Info         | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c12        | c12            | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c13        | c13            |
| 10B  | P-Asserted-Identity           | [34] 9.1                         | c4         | c4             | [34] 9.1                         | c5         | c5             |
| 10C  | P-Charging-Function-Addresses | [52] 4.5,<br>[52A] 4             | c10        | c10            | [52] 4.5,<br>[52A] 4             | c11        | c11            |
| 10D  | P-Charging-Vector             | [52] 4.6,<br>[52A] 4             | c8         | n/a            | [52] 4.6,<br>[52A] 4             | c9         | n/a            |
| 10F  | P-Preferred-Identity          | [34] 9.2                         | x          | x              | [34] 9.2                         | c3         | n/a            |
| 10G  | Privacy                       | [33] 4.2                         | c6         | c6             | [33] 4.2                         | c7         | c7             |
| 10H  | Require                       | [26] 20.32                       | m          | m              | [26] 20.32                       | c14        | c14            |
| 10I  | Server                        | [26] 20.35                       | m          | m              | [26] 20.35                       | i          | i              |
| 10J  | Session-ID                    | [162]                            | c21        | c21            | [162]                            | c21        | c21            |
| 11   | Timestamp                     | [26] 20.38                       | m          | m              | [26] 20.38                       | i          | i              |
| 12   | To                            | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 12A  | User-Agent                    | [26] 20.41                       | m          | m              | [26] 20.41                       | i          | i              |
| 12B  | User-to-User                  | [126] 7                          | c17        | c17            | [126] 7                          | c18        | c18            |
| 13   | Via                           | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 14   | Warning                       | [26] 20.43                       | m          | m              | [26] 20.43                       | i          | i              |

|      |   |
|------|---|
| c1:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c2:  | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.   |
| c3:  | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.   |
| c4:  | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c5:  | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |
| c6:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c7:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c8:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c9:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c10: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c11: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c12: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c13: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c14: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c15: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c16: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c17: | IF A.162/86 THEN m - - transporting user to user information for call centers using SIP.  |
| c18: | IF A.162/86 THEN i - - transporting user to user information for call centers using SIP.  |
| c21: | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.171: Supported header fields within the BYE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Accept-Resource-Priority   | [116] 3.2  | c4         | c4             | [116] 3.2  | c4         | c4             |
| 0B   | Allow-Events   | [28] 7.2.2 | m          | m              | [28] 7.2.2 | i          | c1             |
| 1    | Authentication-Info  | [26] 20.6  | m          | m              | [26] 20.6  | i          | i              |
| 2    | Record-Route   | [26] 20.30 | m          | m              | [26] 20.30 | c3         | c3             |
| 5    | Supported  | [26] 20.37 | m          | m              | [26] 20.37 | i          | i              |
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.   |            |            |                |            |            |                |
| c3:  | IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing.   |            |            |                |            |            |                |
| c4:  | IF A.162/80B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol. |            |            |                |            |            |                |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.171A: Supported header fields within the BYE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | m          | m              | [26] 20.18 | i          | i              |

Prerequisite A.163/3 - BYE response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.172: Supported header fields within the BYE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | c1         | c1             |
| c1:  | IF A.162/19E THEN m ELSE i - - deleting Contact headers. |            |            |                |            |            |                |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.173: Supported header fields within the BYE response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 8    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.174: Supported header fields within the BYE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |

**Table A.175: Void**

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.176: Supported header fields within the BYE response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 6    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.177: Supported header fields within the BYE response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1 | m          | m              | [26] 20.1 | i          | i              |
| 2    | Accept-Encoding | [26] 20.2 | m          | m              | [26] 20.2 | i          | i              |
| 3    | Accept-Language | [26] 20.3 | m          | m              | [26] 20.3 | i          | i              |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.177A: Supported header fields within the BYE response**

| Item | Header field   | Sending   |            |                | Receiving |            |                |
|------|--|-----------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority   | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.162/80B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.178: Supported header fields within the BYE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | c3         | c3             |
| c3:  | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. |            |            |                |            |            |                |

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.178A: Supported header fields within the BYE response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | c1         | c1             | [48] 2    | n/a        | n/a            |
| c1:  | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

**Table A.179: Void**

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/6 - - Additional for 200 (OK) response

**Table A.180: Supported message bodies within the BYE response**

| Item | Header  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | VoiceXML expr / namelist data   | [145] 4.2 | o          | c1             | [145] 4.2 | o          | c1             |
| c1:  | IF A.162/94 THEN o ELSE n/a - - SIP Interface to VoiceXML Media Services. |           |            |                |           |            |                |

## A.2.2.4.4 CANCEL method

Prerequisite A.163/4 - - CANCEL request

Table A.181: Supported header fields within the CANCEL request

| Item  | Header field   | Sending    |            |                | Receiving  |            |                |
|-------|--|------------|------------|----------------|------------|------------|----------------|
|       |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1     | Accept-Contact   | [56B] 9.2  | c10        | c10            | [56B] 9.2  | c11        | c11            |
| 5     | Authorization  | [26] 20.7  | m          | m              | [26] 20.7  | i          | i              |
| 6     | Call-ID  | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 8     | Content-Length   | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 9     | CSeq   | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 10    | Date   | [26] 20.17 | m          | m              | [26] 20.17 | c2         | c2             |
| 11    | From   | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 11A   | Max-Breadth  | [117] 5.8  | c15        | c15            | [117] 5.8  | c16        | c16            |
| 12    | Max-Forwards   | [26] 20.22 | m          | m              | [26] 20.22 | m          | m              |
| 14    | Privacy  | [33] 4.2   | c3         | c3             | [33] 4.2   | c4         | c4             |
| 15    | Reason   | [34A] 2    | c8         | c8             | [34A] 2    | c9         | c9             |
| 16    | Record-Route   | [26] 20.30 | m          | m              | [26] 20.30 | c7         | c7             |
| 17    | Reject-Contact   | [56B] 9.2  | c10        | c10            | [56B] 9.2  | c11        | c11            |
| 17A   | Request-Disposition  | [56B] 9.1  | c10        | c10            | [56B] 9.1  | c11        | c11            |
| 17B   | Resource-Priority  | [116] 3.1  | c12        | c12            | [116] 3.1  | c12        | c12            |
| 18    | Route  | [26] 20.34 | m          | m              | [26] 20.34 | m          | m              |
| 18A   | Session-ID   | [162]      | c17        | c17            | [162]      | c17        | c17            |
| 19    | Supported  | [26] 20.37 | m          | m              | [26] 20.37 | c6         | c6             |
| 20    | Timestamp  | [26] 20.38 | m          | m              | [26] 20.38 | i          | i              |
| 21    | To   | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 22    | User-Agent   | [26] 20.41 | m          | m              | [26] 20.41 | i          | i              |
| 23    | Via  | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c2:   | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.  |            |            |                |            |            |                |
| c3:   | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |            |            |                |            |            |                |
| c4:   | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. |            |            |                |            |            |                |
| c6:   | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.   |            |            |                |            |            |                |
| c7:   | IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.  |            |            |                |            |            |                |
| c8:   | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.   |            |            |                |            |            |                |
| c9:   | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.   |            |            |                |            |            |                |
| c10:  | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.  |            |            |                |            |            |                |
| c11:  | IF A.162/50 THEN i ELSE n/a - - caller preferences for the session initiation protocol.  |            |            |                |            |            |                |
| c12:  | IF A.162/80B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.   |            |            |                |            |            |                |
| c15:  | IF A.162/81 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.  |            |            |                |            |            |                |
| c16:  | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, forking of initial requests.     |            |            |                |            |            |                |
| c17:  | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.  |            |            |                |            |            |                |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.   |            |            |                |            |            |                |

Prerequisite A.163/4 - - CANCEL request

Table A.182: Supported message bodies within the CANCEL request

| Item | Header   | Sending |            |                | Receiving |            |                |
|------|--|---------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | XML Schema for PSTN  | [11B]   |            | c1             | [11B]     |            | i              |
| c1:  | A.3/3 OR A.3/4 OR A.3/5 OR A.3/7C OR A.3/9A OR A.3/10 OR A.3/11 OR A.3/13A THEN m ELSE n/a - - I-CSCF, S-CSCF, BGCF, AS acting as proxy, IBCF (THIG), additional routing functionality, E-CSCF, ISC gateway function (THIG). |         |            |                |           |            |                |

Prerequisite A.163/5 - - CANCEL response for all status-codes

**Table A.183: Supported header fields within the CANCEL response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID  | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length   | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq   | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date   | [26] 20.17 | m          | m              | [26] 20.17 | c1         | c1             |
| 5    | From   | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 5B   | Privacy  | [33] 4.2   | c2         | c2             | [33] 4.2   | c3         | c3             |
| 5C   | Session-ID   | [162]      | c6         | c6             | [162]      | c6         | c6             |
| 6    | Timestamp  | [26] 20.38 | m          | m              | [26] 20.38 | i          | i              |
| 7    | To   | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7A   | User-Agent   | [26] 20.41 | o          |                | [26] 20.41 | o          |                |
| 8    | Via  | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| 9    | Warning  | [26] 20.43 | m          | m              | [26] 20.43 | i          | i              |
| c1:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.  |            |            |                |            |            |                |
| c2:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).   |            |            |                |            |            |                |
| c3:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently. |            |            |                |            |            |                |
| c6:  | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.  |            |            |                |            |            |                |

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.184: Supported header fields within the CANCEL response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Accept-Resource-Priority   | [116] 3.2  | c4         | c4             | [116] 3.2  | c4         | c4             |
| 2    | Record-Route   | [26] 20.30 | m          | m              | [26] 20.30 | c3         | c3             |
| 4    | Supported  | [26] 20.37 | m          | m              | [26] 20.37 | i          | i              |
| c3:  | IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing.   |            |            |                |            |            |                |
| c4:  | IF A.162/80B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol. |            |            |                |            |            |                |



Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.184A: Supported header fields within the CANCEL response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | m          | m              | [26] 20.18 | i          | i              |

**Table A.185: Void**

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.186: Supported header fields within the CANCEL response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.186A: Supported header fields within the CANCEL response**

| Item | Header field   | Sending   |            |                | Receiving |            |                |
|------|--|-----------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority   | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.162/80B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

**Table A.187: Void**

**Table A.188: Void**

Prerequisite A.163/5 - - CANCEL response

**Table A.189: Supported message bodies within the CANCEL response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

A.2.2.4.5 COMET method

Void

A.2.2.4.6 INFO method

Prerequisite A.163/9A - - INFO request

**Table A.190: Supported header fields within the INFO request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | m          | m              | [26] 20.1            | i          | i              |
| 2    | Accept-Encoding               | [26] 20.2            | m          | m              | [26] 20.2            | i          | i              |
| 3    | Accept-Language               | [26] 20.3            | m          | m              | [26] 20.3            | i          | i              |
| 4    | Allow                         | [26] 20.5            | m          | m              | [50] 10              | i          | i              |
| 5    | Allow-Events                  | [28] 7.2.2           | m          | m              | [28] 7.2.2           | c1         | c1             |
| 6    | Authorization                 | [26] 20.7            | m          | m              | [26] 20.7            | i          | i              |
| 7    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 7A   | Call-Info                     | [26] 20.9            | m          | m              | [26] 20.9            | c3         | c3             |
| 9    | Content-Disposition           | [26] 20.11           | m          | m              | [26] 20.11           | i          | i              |
| 10   | Content-Encoding              | [26] 20.12           | m          | m              | [26] 20.12           | i          | i              |
| 11   | Content-Language              | [26] 20.13           | m          | m              | [26] 20.13           | i          | i              |
| 12   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 13   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | i          | i              |
| 14   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 15   | Date                          | [26] 20.17           | m          | m              | [26] 20.17           | c2         | c2             |
| 16   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 17   | Geolocation                   | [89] 4.1             | c36        | c36            | [89] 4.1             | c37        | c37            |
| 17A  | Geolocation-Routing           | [89] 4.1             | c36        | c36            | [89] 4.1             | c37        | c37            |
| 18   | Info-Package                  | [25] 7.2             | c50        | c50            | [25] 7.2             | c51        | c51            |
| 19   | Max-Breadth                   | [117] 5.8            | c48        | c48            | [117] 5.8            | c49        | c49            |
| 20   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | m          | m              |
| 21   | MIME-Version                  | [26] 20.24           | m          | m              | [26] 20.24           | i          | i              |
| 22   | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c23        | c23            | [52] 4.4,<br>[234] 2 | c24        | c24            |
| 23   | P-Charging-Function-Addresses | [52] 4.5             | c21        | c21            | [52] 4.5             | c22        | c22            |
| 24   | P-Charging-Vector             | [52] 4.6             | c19        | c19            | [52] 4.6             | c20        | c20            |
| 26   | Privacy                       | [33] 4.2             | c12        | c12            | [33] 4.2             | c13        | c13            |
| 27   | Proxy-Authorization           | [26] 20.28           | m          | m              | [26] 20.28           | c8         | c8             |
| 28   | Proxy-Require                 | [26] 20.29           | m          | m              | [26] 20.29           | m          | m              |
| 29   | Reason                        | [34A] 2              | c26        | c26            | [34A] 2              | c27        | c27            |
| 30   | Record-Route                  | [26] 20.30           | m          | m              | [26] 20.30           | c7         | c7             |
| 31   | Referred-By                   | [59] 3               | c30        | c30            | [59] 3               | c31        | c31            |
| 33   | Request-Disposition           | [56B] 9.1            | c28        | c28            | [56B] 9.1            | c28        | c28            |
| 34   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | c5         | c5             |
| 35   | Resource-Priority             | [116] 3.1            | c38        | c38            | [116] 3.1            | c38        | c38            |
| 36   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | m          | m              |
| 37   | Security-Client               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c25        | c25            |
| 38   | Security-Verify               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c25        | c25            |
| 38A  | Session-ID                    | [162]                | c52        | c52            | [162]                | c52        | c52            |
| 39   | Subject                       | [26] 20.36           | m          | m              | [26] 20.36           | i          | i              |
| 40   | Supported                     | [26] 20.37           | m          | m              | [26] 20.37           | c6         | c6             |
| 41   | Timestamp                     | [26] 20.38           | m          | m              | [26] 20.38           | i          | i              |
| 42   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 43   | User-Agent                    | [26] 20.41           | m          | m              | [26] 20.41           | i          | i              |
| 44   | Via                           | [26] 20.42           | m          | m              | [26] 20.42           | m          | m              |

|       |   |
|-------|---|
| c1:   | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |
| c2:   | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c3:   | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |
| c5:   | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6:   | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.  |
| c7:   | IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.   |
| c8:   | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.  |
| c12:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c13:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c19:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c20:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c21:  | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c22:  | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c23:  | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c24:  | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c25:  | IF A.162/47 OR A.162/47A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |
| c26:  | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c27:  | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c28:  | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c30:  | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.  |
| c31:  | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c36:  | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c37:  | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c38:  | IF A.162/80A THEN m ELSE n/a - - inclusion of INFO, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.  |
| c48:  | IF A.162/81 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |
| c49:  | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, forking of initial requests.  |
| c50:  | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |
| c51:  | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |
| c52:  | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.  |

Prerequisite A.163/9A - - INFO request

**Table A.191: Supported message bodies within the INFO request**

| Item | Header       | Sending |            |                | Receiving |            |                |
|------|--------------|---------|------------|----------------|-----------|------------|----------------|
|      |              | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Info-Package | [25]    | m          | m              | [25]      | i          | i              |

Prerequisite A.163/9B - - INFO response

Prerequisite: A.164/1 - - Additional for 100 (Trying) response

**Table A.192: Supported header fields within the INFO response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID   | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length  | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq  | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date  | [26] 20.17 | c1         | c1             | [26] 20.17 | c2         | c2             |
| 5    | From  | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To  | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies. |            |            |                |            |            |                |
| c2:  | IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.   |            |            |                |            |            |                |

Prerequisite A.163/9B - - INFO response for all remaining status-codes

**Table A.193: Supported header fields within the INFO response**

| Item | Header field  | Sending                          |            |                | Receiving                        |            |                |
|------|---|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |   | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow   | [26] 20.5                        | m          | m              | [26] 20.5                        | i          | i              |
| 1    | Call-ID   | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 2    | Call-Info   | [26] 20.9                        | m          | m              | [26] 20.9                        | c3         | c3             |
| 3    | Content-Disposition   | [26] 20.11                       | m          | m              | [26] 20.11                       | i          | i              |
| 4    | Content-Encoding  | [26] 20.12                       | m          | m              | [26] 20.12                       | i          | i              |
| 5    | Content-Language  | [26] 20.13                       | m          | m              | [26] 20.13                       | i          | i              |
| 6    | Content-Length  | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 7    | Content-Type  | [26] 20.15                       | m          | m              | [26] 20.15                       | i          | i              |
| 8    | CSeq  | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 9    | Date  | [26] 20.17                       | m          | m              | [26] 20.17                       | c1         | c1             |
| 10   | From  | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 11   | Geolocation-Error   | [89] 4.3                         | c17        | c17            | [89] 4.3                         | c18        | c18            |
| 12   | MIME-Version  | [26] 20.24                       | m          | m              | [26] 20.24                       | i          | i              |
| 13   | Organization  | [26] 20.25                       | m          | m              | [26] 20.25                       | c2         | c2             |
| 14   | P-Access-Network-Info   | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c13        | c13            | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c14        | c14            |
| 15   | P-Charging-Function-Addresses   | [52] 4.5,<br>[52A] 4             | c11        | c11            | [52] 4.5,<br>[52A] 4             | c12        | c12            |
| 16   | P-Charging-Vector   | [52] 4.6,<br>[52A] 4             | c9         | n/a            | [52] 4.6,<br>[52A] 4             | c10        | n/a            |
| 18   | Privacy   | [33] 4.2                         | c7         | c7             | [33] 4.2                         | c8         | c8             |
| 19   | Require   | [26] 20.32                       | m          | m              | [26] 20.32                       | c15        | c15            |
| 20   | Server  | [26] 20.35                       | m          | m              | [26] 20.35                       | i          | i              |
| 20A  | Session-ID  | [162]                            | c21        | c21            | [162]                            | c21        | c21            |
| 21   | Timestamp   | [26] 20.38                       | i          | i              | [26] 20.38                       | i          | i              |
| 22   | To  | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 23   | User-Agent  | [26] 20.41                       | m          | m              | [26] 20.41                       | i          | i              |
| 24   | Via   | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 25   | Warning   | [26] 20.43                       | m          | m              | [26] 20.43                       | i          | i              |
| c1:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c2:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |                                  |            |                |                                  |            |                |
| c3:  | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |                                  |            |                |                                  |            |                |
| c7:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |                                  |            |                |                                  |            |                |
| c8:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |                                  |            |                |                                  |            |                |
| c9:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |                                  |            |                |                                  |            |                |
| c10: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c11: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |                                  |            |                |                                  |            |                |
| c12: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |                                  |            |                |                                  |            |                |
| c13: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |                                  |            |                |                                  |            |                |
| c14: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |                                  |            |                |                                  |            |                |
| c15: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |                                  |            |                |                                  |            |                |
| c17: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |                                  |            |                |                                  |            |                |
| c18: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |                                  |            |                |                                  |            |                |
| c21: | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |

Prerequisite A.163/9B - - INFO response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.194: Supported header fields within the INFO response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Accept   | [26] 20.1  | m          | m              | [26] 20.1  | i          | i              |
| 2    | Accept-Encoding  | [26] 20.2  | m          | m              | [26] 20.2  | i          | i              |
| 3    | Accept-Language  | [26] 20.3  | m          | m              | [26] 20.3  | i          | i              |
| 4    | Accept-Resource-Priority   | [116] 3.2  | c4         | c4             | [116] 3.2  | c4         | c4             |
| 5    | Allow-Events   | [28] 7.2.2 | m          | m              | [28] 7.2.2 | c1         | c1             |
| 6    | Authentication-Info  | [26] 20.6  | m          | m              | [26] 20.6  | i          | i              |
| 9    | Supported  | [26] 20.37 | m          | m              | [26] 20.37 | i          | i              |
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.   |            |            |                |            |            |                |
| c4:  | IF A.162/80A THEN m ELSE n/a - - inclusion of INFO, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol. |            |            |                |            |            |                |

Prerequisite A.163/9B - - INFO response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.195: Supported header fields within the INFO response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | m          | m              | [26] 20.18 | i          | i              |

Prerequisite A.163/9B - - INFO response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.195A: Void**

| Item | Header field | Sending |            |                | Receiving |            |                |
|------|--------------|---------|------------|----------------|-----------|------------|----------------|
|      |              | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
|      |              |         |            |                |           |            |                |

Prerequisite A.163/9B - - INFO response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.196: Supported header fields within the INFO response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 6    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/9B - - INFO response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table 197: Supported header fields within the INFO response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |

**Table A.198: Void**

Prerequisite A.163/9B - - INFO response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type)

**Table A.199: Supported header fields within the INFO response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1 | m          | m              | [26] 20.1 | i          | i              |
| 2    | Accept-Encoding | [26] 20.2 | m          | m              | [26] 20.2 | i          | i              |
| 3    | Accept-Language | [26] 20.3 | m          | m              | [26] 20.3 | i          | i              |

Prerequisite A.163/9B - - INFO response

Prerequisite: A.164/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.199A: Supported header fields within the INFO response**

| Item | Header field   | Sending   |            |                | Receiving |            |                |
|------|--|-----------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority   | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.162/80A THEN m ELSE n/a - - inclusion of INFO, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.163/9B - - INFO response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.200: Supported header fields within the INFO response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | c3         | c3             |
| c3:  | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. |            |            |                |            |            |                |



Prerequisite A.163/9B - - INFO response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.200A: Supported header fields within the INFO response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | c1         | c1             | [48] 2    | n/a        | n/a            |
| c1:  | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

**Table A.201: Void**

**Table A.202: Void**

Prerequisite A.163/9B - - INFO response

**Table A.203: Supported message bodies within the INFO response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

#### A.2.2.4.7 INVITE method

Prerequisite A.163/8 - - INVITE request

**Table A.204: Supported header fields within the INVITE request**

| Item | Header field                  | Sending                  |            |                | Receiving                |            |                |
|------|-------------------------------|--------------------------|------------|----------------|--------------------------|------------|----------------|
|      |                               | Ref.                     | RFC status | Profile status | Ref.                     | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1                | m          | m              | [26] 20.1                | i          | i              |
| 1A   | Accept-Contact                | [56B] 9.2                | c34        | c34            | [56B] 9.2                | c34        | c35            |
| 2    | Accept-Encoding               | [26] 20.2                | m          | m              | [26] 20.2                | i          | i              |
| 3    | Accept-Language               | [26] 20.3                | m          | m              | [26] 20.3                | i          | i              |
| 4    | Alert-Info                    | [26] 20.4                | c2         | c2             | [26] 20.4                | c3         | c3             |
| 5    | Allow                         | [26] 20.5                | m          | m              | [26] 20.5                | i          | i              |
| 6    | Allow-Events                  | [28] 7.2.2               | m          | m              | [28] 7.2.2               | c1         | c1             |
| 7    | Answer-Mode                   | [158]                    | c67        | c67            | [158]                    | c68        | c68            |
| 8    | Authorization                 | [26] 20.7                | m          | m              | [26] 20.7                | i          | i              |
| 9    | Call-ID                       | [26] 20.8                | m          | m              | [26] 20.8                | m          | m              |
| 10   | Call-Info                     | [26] 20.9                | m          | m              | [26] 20.9                | c12        | c12            |
| 11   | Contact                       | [26] 20.10               | m          | m              | [26] 20.10               | i          | i              |
| 12   | Content-Disposition           | [26] 20.11               | m          | m              | [26] 20.11               | i          | c6             |
| 13   | Content-Encoding              | [26] 20.12               | m          | m              | [26] 20.12               | i          | c6             |
| 14   | Content-Language              | [26] 20.13               | m          | m              | [26] 20.13               | i          | c6             |
| 15   | Content-Length                | [26] 20.14               | m          | m              | [26] 20.14               | m          | m              |
| 16   | Content-Type                  | [26] 20.15               | m          | m              | [26] 20.15               | i          | c6             |
| 17   | CSeq                          | [26] 20.16               | m          | m              | [26] 20.16               | m          | m              |
| 18   | Date                          | [26] 20.17               | m          | m              | [26] 20.17               | c4         | c4             |
| 19   | Expires                       | [26] 20.19               | m          | m              | [26] 20.19               | i          | i              |
| 19A  | Feature-Caps                  | [190]                    | c73        | c73            | [190]                    | c73        | c73            |
| 20   | From                          | [26] 20.20               | m          | m              | [26] 20.20               | m          | m              |
| 20A  | Geolocation                   | [89] 4.1                 | c47        | c47            | [89] 4.1                 | c48        | c48            |
| 20B  | Geolocation-Routing           | [89] 4.1                 | c47        | c47            | [89] 4.1                 | c48        | c48            |
| 20C  | History-Info                  | [66] 4.1                 | c43        | c43            | [66] 4.1                 | c43        | c43            |
| 21   | In-Reply-To                   | [26] 20.21               | m          | m              | [26] 20.21               | i          | i              |
| 21A  | Join                          | [61] 7.1                 | c41        | c41            | [61] 7.1                 | c42        | c42            |
| 21B  | Max-Breadth                   | [117] 5.8                | c63        | c63            | [117] 5.8                | c64        | c64            |
| 22   | Max-Forwards                  | [26] 20.22               | m          | m              | [26] 20.22               | m          | m              |
| 23   | MIME-Version                  | [26] 20.24               | m          | m              | [26] 20.24               | i          | c6             |
| 23A  | Min-SE                        | [58] 5                   | o          | o              | [58] 5                   | o          | o              |
| 24   | Organization                  | [26] 20.25               | m          | m              | [26] 20.25               | c5         | c5             |
| 24A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2     | c28        | c28            | [52] 4.4,<br>[234] 2     | c29        | c30            |
| 24B  | P-Asserted-Identity           | [34] 9.1                 | c15        | c15            | [34] 9.1                 | c16        | c16            |
| 24C  | P-Asserted-Service            | [121] 4.1                | c53        | c53            | [121] 4.1                | c54        | c54            |
| 24D  | P-Called-Party-ID             | [52] 4.2                 | c19        | c19            | [52] 4.2                 | c20        | c21            |
| 24E  | P-Charging-Function-Addresses | [52] 4.5                 | c26        | c27            | [52] 4.5                 | c26        | c27            |
| 24F  | P-Charging-Vector             | [52] 4.6                 | c24        | c24            | [52] 4.6                 | c25        | c25            |
| 24H  | P-Early-Media                 | [109] 8                  | o          | c50            | [109] 8                  | o          | c51            |
| 25   | P-Media-Authorization         | [31] 5.1                 | c9         | x              | [31] 5.1                 | n/a        | n/a            |
| 25A  | P-Preferred-Identity          | [34] 9.2                 | x          | c69            | [34] 9.2                 | c14        | c14            |
| 25B  | P-Preferred-Service           | [121] 4.2                | x          | x              | [121] 4.2                | c52        | c52            |
| 25C  | P-Private-Network-Indication  | [134]                    | c59        | c59            | [134]                    | c59        | c59            |
| 25D  | P-Profile-Key                 | [97] 5                   | c45        | c45            | [97] 5                   | c46        | c46            |
| 25E  | P-Served-User                 | [133] 6                  | c60        | c60            | [133] 6                  | c60        | c60            |
| 25F  | P-User-Database               | [82] 4                   | c44        | c44            | [82] 4                   | c44        | c44            |
| 25G  | P-Visited-Network-ID          | [52] 4.3                 | c22        | n/a            | [52] 4.3                 | c23        | n/a            |
| 26   | Priority                      | [26] 20.26               | m          | m              | [26] 20.26               | i          | i              |
| 26A  | Privacy                       | [33] 4.2                 | c17        | c17            | [33] 4.2                 | c18        | c18            |
| 26B  | Priv-Answer-Mode              | [158]                    | c67        | c67            | [158]                    | c68        | c68            |
| 27   | Proxy-Authorization           | [26] 20.28               | m          | m              | [26] 20.28               | c13        | c13            |
| 28   | Proxy-Require                 | [26]<br>20.29,<br>[34] 4 | m          | m              | [26]<br>20.29,<br>[34] 4 | m          | m              |
| 28A  | Reason                        | [34A] 2                  | c32        | c32            | [34A] 2                  | c33        | c33            |
| 29   | Record-Route                  | [26] 20.30               | m          | m              | [26] 20.30               | c11        | c11            |
| 29A  | Recv-Info                     | [25] 5.2.3               | c65        | c65            | [25] 5.2.3               | c66        | c66            |
| 30   | Referred-By                   | [59] 3                   | c37        | c37            | [59] 3                   | c38        | c38            |
| 31   | Reject-Contact                | [56B] 9.2                | c34        | c34            | [56B] 9.2                | c34        | c35            |
| 31A  | Replaces                      | [60] 6.1                 | c39        | c39            | [60] 6.1                 | c40        | c40            |

| Item | Header field        | Sending         |            |                | Receiving       |            |                |
|------|---------------------|-----------------|------------|----------------|-----------------|------------|----------------|
|      |                     | Ref.            | RFC status | Profile status | Ref.            | RFC status | Profile status |
| 31B  | Reply-To            | [26] 20.31      | m          | m              | [26] 20.31      | i          | i              |
| 31C  | Request-Disposition | [56B] 9.1       | c34        | c34            | [56B] 9.1       | c34        | c34            |
| 32   | Require             | [26] 20.32      | m          | m              | [26] 20.32      | c7         | c7             |
| 32A  | Resource-Priority   | [116] 3.1       | c49        | c49            | [116] 3.1       | c49        | c49            |
| 33   | Route               | [26] 20.34      | m          | m              | [26] 20.34      | m          | m              |
| 33A  | Security-Client     | [48] 2.3.1      | x          | x              | [48] 2.3.1      | c31        | c31            |
| 33B  | Security-Verify     | [48] 2.3.1      | x          | x              | [48] 2.3.1      | c31        | c31            |
|      |                     |                 |            |                |                 |            |                |
| 33D  | Session-Expires     | [58] 4          | c36        | c36            | [58] 4          | c36        | c36            |
| 33E  | Session-ID          | [162]           | c70        | c70            | [162]           | c70        | c70            |
| 34   | Subject             | [26] 20.36      | m          | m              | [26] 20.36      | i          | i              |
| 35   | Supported           | [26] 20.37      | m          | m              | [26] 20.37      | c8         | c8             |
| 35A  | Target-Dialog       | [184] 7         | c71        | c71            | [184] 7         | c72        | c72            |
| 36   | Timestamp           | [26] 20.38      | m          | m              | [26] 20.38      | i          | i              |
| 37   | To                  | [26] 20.39      | m          | m              | [26] 20.39      | m          | m              |
| 37A  | Trigger-Consent     | [125]<br>5.11.2 | c55        | c55            | [125]<br>5.11.2 | c56        | c56            |
| 38   | User-Agent          | [26] 20.41      | m          | m              | [26] 20.41      | i          | i              |
| 38A  | User-to-User        | [126] 7         | c57        | c57            | [126] 7         | c58        | c58            |
| 39   | Via                 | [26] 20.42      | m          | m              | [26] 20.42      | m          | m              |

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |         |            |                |           |            |                |
| c2:  | IF A.162/10 THEN n/a ELSE m - - suppression or modification of alerting information data.   |         |            |                |           |            |                |
| c3:  | IF A.162/10 THEN m ELSE i - - suppression or modification of alerting information data.   |         |            |                |           |            |                |
| c4:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |         |            |                |           |            |                |
| c5:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |         |            |                |           |            |                |
| c6:  | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.   |         |            |                |           |            |                |
| c7:  | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.             |         |            |                |           |            |                |
| c8:  | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.  |         |            |                |           |            |                |
| c9:  | IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization.   |         |            |                |           |            |                |
| c11: | IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.   |         |            |                |           |            |                |
| c12: | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |         |            |                |           |            |                |
| c13: | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.  |         |            |                |           |            |                |
| c14: | IF A.162/30A OR A.162/30C THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity, act as entity passing on identity transparently independent of trust domain.   |         |            |                |           |            |                |
| c15: | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |         |            |                |           |            |                |
| c16: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.   |         |            |                |           |            |                |
| c17: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |         |            |                |           |            |                |
| c18: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |         |            |                |           |            |                |
| c19: | IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension.   |         |            |                |           |            |                |
| c20: | IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension.   |         |            |                |           |            |                |
| c21: | IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND (A.3/3 OR A.3/9A) THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or (I-CSCF or IBCF (THIG)).   |         |            |                |           |            |                |
| c22: | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension.  |         |            |                |           |            |                |
| c23: | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response.   |         |            |                |           |            |                |
| c24: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |         |            |                |           |            |                |
| c25: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |         |            |                |           |            |                |
| c26: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |         |            |                |           |            |                |
| c27: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.   |         |            |                |           |            |                |
| c28: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.  |         |            |                |           |            |                |
| c29: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.  |         |            |                |           |            |                |
| c30: | IF A.162/43 OR (A.162/41 AND A.3/2) THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension (with or without P-CSCF). |         |            |                |           |            |                |
| c31: | IF A.162/47 OR A.162/47A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |         |            |                |           |            |                |
| c32: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |         |            |                |           |            |                |
| c33: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.  |         |            |                |           |            |                |
| c34: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |         |            |                |           |            |                |
| c35: | IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CSCF.   |         |            |                |           |            |                |
| c36: | IF A.162/52 THEN m ELSE n/a - - the SIP session timer.  |         |            |                |           |            |                |
| c37: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.  |         |            |                |           |            |                |
| c38: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |         |            |                |           |            |                |
| c39: | IF A.162/54 THEN m ELSE n/a - - the Session Initiation Protocol (SIP) "Replaces" header.  |         |            |                |           |            |                |
| c40: | IF A.162/54 THEN i ELSE n/a - - the Session Initiation Protocol (SIP) "Replaces" header.  |         |            |                |           |            |                |

| Item  | Header field   | Sending |            |                | Receiving |            |                |
|-------|--|---------|------------|----------------|-----------|------------|----------------|
|       |  | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| c41:  | IF A.162/55 THEN m ELSE n/a  | --      |            |                |           |            |                |
| c42:  | IF A.162/55 THEN i ELSE n/a  | --      |            |                |           |            |                |
| c43:  | IF A.162/57 THEN m ELSE n/a  | --      |            |                |           |            |                |
| c44:  | IF A.162/60 THEN m ELSE n/a  | --      |            |                |           |            |                |
| c45:  | IF A.162/66A THEN m ELSE n/a   | --      |            |                |           |            |                |
| c46:  | IF A.162/66B THEN m ELSE n/a   | --      |            |                |           |            |                |
| c47:  | IF A.162/70 THEN m ELSE n/a  | --      |            |                |           |            |                |
| c48:  | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a  | --      |            |                |           |            |                |
| c49:  | IF A.162/80 THEN m ELSE n/a  | --      |            |                |           |            |                |
| c50:  | IF A.162/76 THEN m ELSE n/a  | --      |            |                |           |            |                |
| c51:  | IF A.162/76 THEN (IF A.3/2 THEN m ELSE i) ELSE n/a   | --      |            |                |           |            |                |
| c52:  | IF A.162/84A THEN m ELSE n/a   | --      |            |                |           |            |                |
| c53:  | IF A.162/84 THEN m ELSE n/a  | --      |            |                |           |            |                |
| c54:  | IF A.162/84 OR A.162/30B THEN m ELSE i   | --      |            |                |           |            |                |
| c55:  | IF A.162/85 THEN m ELSE n/a  | --      |            |                |           |            |                |
| c56:  | IF A.162/85 THEN i ELSE n/a  | --      |            |                |           |            |                |
| c57:  | IF A.162/86 THEN m   | --      |            |                |           |            |                |
| c58:  | IF A.162/86 THEN i   | --      |            |                |           |            |                |
| c59:  | IF A.162/87 THEN m ELSE n/a  | --      |            |                |           |            |                |
| c60:  | IF A.162/88 THEN m   | --      |            |                |           |            |                |
| c63:  | IF A.162/81 THEN m ELSE n/a  | --      |            |                |           |            |                |
| c64:  | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a  | --      |            |                |           |            |                |
| c65:  | IF A.162/20 THEN m ELSE n/a  | --      |            |                |           |            |                |
| c66:  | IF A.162/20 THEN i ELSE n/a  | --      |            |                |           |            |                |
| c67:  | IF A.162/97 THEN m ELSE n/a  | --      |            |                |           |            |                |
| c68:  | IF NOT A.162/97 THEN n/a ELSE IF A.162/97A THEN m ELSE i   | --      |            |                |           |            |                |
| c69:  | IF A.162/30C THEN m ELSE x   | --      |            |                |           |            |                |
| c70:  | IF A.162/101 THEN m ELSE n/a   | --      |            |                |           |            |                |
| c71:  | IF A.162/109 THEN m ELSE n/a   | --      |            |                |           |            |                |
| c72:  | IF A.162/109 THEN i ELSE n/a   | --      |            |                |           |            |                |
| c73:  | IF A.162/110 THEN m ELSE n/a   | --      |            |                |           |            |                |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. |         |            |                |           |            |                |

Prerequisite A.163/8 -- INVITE request

**Table A.205: Supported message bodies within the INVITE request**

| Item | Header  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | XML Schema for PSTN   | [11B]   |            | c1             | [11B]     |            | i              |
| 2    | application/vnd.3gpp.ussd   | [8W]    |            | m              | [8W]      |            | i              |
| c1:  | A.3/3 OR A.3/4 OR A.3/5 OR A.3/7C OR A.3/9A OR A.3/10 OR A.3/11 OR A.3/13A THEN m ELSE n/a -- I-CSCF, S-CSCF, BGCF, AS acting as proxy, IBCF (THIG), additional routing functionality, E-CSCF, ISC gateway function (THIG). |         |            |                |           |            |                |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/1 - - Additional for 100 (Trying) response

**Table A.206: Supported header fields within the INVITE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID   | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length  | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq  | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date  | [26] 20.17 | c1         | c1             | [26] 20.17 | c2         | c2             |
| 5    | From  | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To  | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies. |            |            |                |            |            |                |
| c2:  | IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.   |            |            |                |            |            |                |

Prerequisite A.163/9 - - INVITE response for all remaining status-codes

**Table A.207: Supported header fields within the INVITE response**



| Item | Header field                  | Sending                          |            |                | Receiving                        |            |                |
|------|-------------------------------|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |                               | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow                         | [26] 20.5                        | m          | m              | [26] 20.5                        | i          | i              |
| 1    | Call-ID                       | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 1A   | Call-Info                     | [26] 20.9                        | m          | m              | [26] 20.9                        | c4         | c4             |
| 2    | Content-Disposition           | [26] 20.11                       | m          | m              | [26] 20.11                       | i          | c3             |
| 3    | Content-Encoding              | [26] 20.12                       | m          | m              | [26] 20.12                       | i          | c3             |
| 4    | Content-Language              | [26] 20.13                       | m          | m              | [26] 20.13                       | i          | c3             |
| 5    | Content-Length                | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6    | Content-Type                  | [26] 20.15                       | m          | m              | [26] 20.15                       | i          | c3             |
| 7    | CSeq                          | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8    | Date                          | [26] 20.17                       | m          | m              | [26] 20.17                       | c1         | c1             |
| 8A   | Expires                       | [26] 20.19                       | m          | m              | [26] 20.19                       | i          | i              |
| 9    | From                          | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A   | Geolocation-Error             | [89] 4.3                         | c24        | c24            | [89] 4.3                         | c24        | c24            |
| 9B   | History-Info                  | [66] 4.1                         | c17        | c17            | [66] 4.1                         | c17        | c17            |
| 10   | MIME-Version                  | [26] 20.24                       | m          | m              | [26] 20.24                       | i          | c3             |
| 11   | Organization                  | [26] 20.25                       | m          | m              | [26] 20.25                       | c2         | c2             |
| 11A  | P-Access-Network-Info         | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c14        | c14            | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c15        | c15            |
| 11B  | P-Asserted-Identity           | [34] 9.1                         | c6         | c6             | [34] 9.1                         | c7         | c7             |
| 11C  | P-Charging-Function-Addresses | [52] 4.5,<br>[52A] 4             | c12        | c12            | [52] 4.5,<br>[52A] 4             | c13        | c13            |
| 11D  | P-Charging-Vector             | [52] 4.6,<br>[52A] 4             | c10        | c10            | [52] 4.6,<br>[52A] 4             | c11        | c11            |
| 11F  | P-Preferred-Identity          | [34] 9.2                         | x          | x              | [34] 9.2                         | c5         | n/a            |
| 11G  | Privacy                       | [33] 4.2                         | c8         | c8             | [33] 4.2                         | c9         | c9             |
| 11H  | Reply-To                      | [26] 20.31                       | m          | m              | [26] 20.31                       | i          | i              |
| 11I  | Require                       | [26] 20.32                       | m          | m              | [26] 20.32                       | c16        | c16            |
| 11J  | Server                        | [26] 20.35                       | m          | m              | [26] 20.35                       | i          | i              |
| 11K  | Session-ID                    | [162]                            | c25        | c25            | [162]                            | c25        | c25            |
| 12   | Timestamp                     | [26] 20.38                       | m          | m              | [26] 20.38                       | i          | i              |
| 13   | To                            | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 13A  | User-Agent                    | [26] 20.41                       | m          | m              | [26] 20.41                       | i          | i              |
| 13B  | User-to-User                  | [126] 7                          | c20        | c20            | [126] 7                          | c21        | c21            |
| 14   | Via                           | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 15   | Warning                       | [26] 20.43                       | m          | m              | [26] 20.43                       | i          | i              |

|      |   |
|------|---|
| c1:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c2:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |
| c3:  | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.   |
| c4:  | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |
| c5:  | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.   |
| c6:  | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c7:  | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |
| c8:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c9:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c10: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c11: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c12: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c13: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c14: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c15: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c16: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c17: | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c18: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c19: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c20: | IF A.162/86 THEN m - - transporting user to user information for call centers using SIP.  |
| c21: | IF A.162/86 THEN i - - transporting user to user information for call centers using SIP.  |
| c24: | IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.  |
| c25: | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/101A - - Additional for 18x response

**Table A.208: Supported header fields within the INVITE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Contact   | [26] 20.10 | m          | m              | [26] 20.10 | i          | i              |
| 4A   | Feature-Caps  | [190]      | c19        | c19            | [190]      | c19        | c19            |
| 5    | P-Answer-State  | [111]      | c13        | c13            | [111]      | c14        | c14            |
| 5A   | P-Early-Media   | [109] 8    | o          | c11            | [109] 8    | o          | c12            |
| 6    | P-Media-Authorization   | [31] 5.1   | c9         | x              | [31] 5.1   | n/a        | n/a            |
| 6A   | Reason  | [130]      | o          | c18            | [130]      | o          | c18            |
| 7    | Record-Route  | [26] 20.30 | m          | m              | [26] 20.30 | c15        | c15            |
| 8    | Recv-Info   | [25] 5.2.3 | c16        | c16            | [25] 5.2.3 | c17        | c17            |
| 9    | RSeq  | [27] 7.1   | m          | m              | [27] 7.1   | i          | i              |
| 11   | Supported   | [26] 20.37 | m          | m              | [26] 20.37 | i          | i              |
| c9:  | IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization.   |            |            |                |            |            |                |
| c11: | IF A.162/76 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.  |            |            |                |            |            |                |
| c12: | IF A.162/76 THEN (IF A.3/2 THEN m ELSE i) ELSE n/a - - P-CSCF, using the information in the P-Early-Media header.   |            |            |                |            |            |                |
| c13: | IF A.162/75 THEN m ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular. |            |            |                |            |            |                |
| c14: | IF A.162/75 THEN i ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular. |            |            |                |            |            |                |
| c15: | IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.   |            |            |                |            |            |                |
| c16: | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |            |            |                |            |            |                |
| c17: | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |            |            |                |            |            |                |
| c18: | IF A.162/48A THEN o ELSE n/a - - use of the Reason header field in Session Initiation Protocol (SIP) responses.   |            |            |                |            |            |                |
| c19: | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.   |            |            |                |            |            |                |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/5A - - Additional for 199 (Early Dialog Terminated) response

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/2 - - Additional for 180 (Ringing) response

**Table A.208A: Supported header fields within the INVITE response**

| Item | Header field | Sending   |            |                | Receiving |            |                |
|------|--------------|-----------|------------|----------------|-----------|------------|----------------|
|      |              | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Alert-Info   | [26] 20.4 | m          | m              | [26] 20.4 | i          | i              |

**Table A.208B: Supported header fields within the INVITE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Contact   | [26] 20.10 | m          | m              | [26] 20.10 | i          | i              |
| 5    | Reason  | [130]      | o          | c18            | [130]      | o          | c18            |
| 7    | Record-Route  | [26] 20.30 | m          | m              | [26] 20.30 | c15        | c15            |
| 8    | Recv-Info   | [25] 5.2.3 | c16        | c16            | [25] 5.2.3 | c17        | c17            |
| 9    | RSeq  | [27] 7.1   | m          | m              | [27] 7.1   | i          | i              |
| 11   | Supported   | [26] 20.37 | m          | m              | [26] 20.37 | i          | i              |
| c15: | IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog. |            |            |                |            |            |                |
| c16: | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |            |            |                |            |            |                |
| c17: | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |            |            |                |            |            |                |
| c18: | IF A.162/48A THEN o ELSE n/a - - use of the Reason header field in Session Initiation Protocol (SIP) responses.       |            |            |                |            |            |                |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.209: Supported header fields within the INVITE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Accept  | [26] 20.1  | m          | m              | [26] 20.1  | i          | i              |
| 1A   | Accept-Encoding   | [26] 20.2  | m          | m              | [26] 20.2  | i          | i              |
| 1B   | Accept-Language   | [26] 20.3  | m          | m              | [26] 20.3  | i          | i              |
| 1C   | Accept-Resource-Priority  | [116] 3.2  | c12        | c12            | [116] 3.2  | c12        | c12            |
| 2    | Allow-Events  | [28] 7.2.2 | m          | m              | [28] 7.2.2 | c1         | c1             |
| 3    | Answer-Mode   | [158]      | c19        | c19            | [158]      | c20        | c20            |
| 4    | Authentication-Info   | [26] 20.6  | m          | m              | [26] 20.6  | i          | i              |
| 6    | Contact   | [26] 20.10 | m          | m              | [26] 20.10 | i          | i              |
| 6A   | Feature-Caps  | [190]      | c22        | c22            | [190]      | c22        | c22            |
| 7    | P-Answer-State  | [111]      | c13        | c13            | [111]      | c14        | c14            |
| 8    | P-Media-Authorization   | [31] 5.1   | c9         | x              | [31] 5.1   | n/a        | n/a            |
| 8A   | Priv-Answer-Mode  | [158]      | c19        | c19            | [158]      | c20        | c20            |
| 9    | Record-Route  | [26] 20.30 | m          | m              | [26] 20.30 | c3         | c3             |
| 9A   | Recv-Info   | [25] 5.2.3 | c17        | c17            | [25] 5.2.3 | c18        | c18            |
| 10   | Session-Expires   | [58] 4     | c11        | c11            | [58] 4     | c11        | c11            |
| 13   | Supported   | [26] 20.37 | m          | m              | [26] 20.37 | i          | i              |
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |            |            |                |            |            |                |
| c3:  | IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.   |            |            |                |            |            |                |
| c9:  | IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization.   |            |            |                |            |            |                |
| c11: | IF A.162/52 THEN m ELSE n/a - - the SIP session timer.  |            |            |                |            |            |                |
| c12: | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.   |            |            |                |            |            |                |
| c13: | IF A.162/75 THEN m ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular.   |            |            |                |            |            |                |
| c14: | IF A.162/75 THEN i ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular.   |            |            |                |            |            |                |
| c17: | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |            |            |                |            |            |                |
| c18: | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |            |            |                |            |            |                |
| c19: | IF A.162/97 THEN m ELSE n/a - - requesting answering modes for SIP.   |            |            |                |            |            |                |
| c20: | IF NOT A.162/97 THEN n/a ELSE IF A.162/97A THEN m ELSE i - - requesting answering modes for SIP, adding, deleting or reading the Answer-Mode header or Priv-Answer-Mode header before proxying the request or response. |            |            |                |            |            |                |
| c22: | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.   |            |            |                |            |            |                |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.209A: Supported header fields within the INVITE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info  | [26] 20.18 | m          | m              | [26] 20.18 | i          | i              |
| 2    | Reason  | [130]      | o          | c1             | [130]      | o          | c1             |
| c1:  | IF A.162/48A THEN o ELSE n/a - - use of the Reason header field in Session Initiation Protocol (SIP) responses. |            |            |                |            |            |                |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.210: Supported header fields within the INVITE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | c1         | c1             |
| c1:  | IF A.162/19E THEN m ELSE i - - deleting Contact headers. |            |            |                |            |            |                |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.211: Supported header fields within the INVITE response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 6    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 15   | WWW-Authenticate   | [26] 20.44 | o          |                | [26] 20.44 | o          |                |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 600 (Busy Everywhere), 603 (Decline) response

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.6/16 - - Additional for 403 (Forbidden) response

**Table A.211A: Supported header fields within the INVITE response**

| Item | Header field   | Sending |            |                | Receiving |            |                |
|------|--|---------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | P-Refused-URI-List   | [183]   | c1         | c1             | [183]     | c1         | c1             |
| c1:  | IF A.162/108 THEN m ELSE n/a -- The SIP P-Refused-URI-List private-header. |         |            |                |           |            |                |

**Table A.212: Supported header fields within the INVITE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 8    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |
| 12   | Via          | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |

**Table A.213: Void**

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.214: Supported header fields within the INVITE response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 6    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 11   | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.215: Supported header fields within the INVITE response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1 | m          | m              | [26] 20.1 | i          | i              |
| 2    | Accept-Encoding | [26] 20.2 | m          | m              | [26] 20.2 | i          | i              |
| 3    | Accept-Language | [26] 20.3 | m          | m              | [26] 20.3 | i          | i              |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.215A: Supported header fields within the INVITE response**

| Item | Header field  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority  | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.216: Supported header fields within the INVITE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 10   | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | c3         | c3             |
| c3:  | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. |            |            |                |            |            |                |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.216A: Supported header fields within the INVITE response**

| Item  | Header field    | Sending |            |                | Receiving |            |                |
|---|-----------------|---------|------------|----------------|-----------|------------|----------------|
|   |                 | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3   | Security-Server | [48] 2  | c1         | c1             | [48] 2    | n/a        | n/a            |
| c1: IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |                 |         |            |                |           |            |                |

Prerequisite A.16/9 - - INVITE response

Prerequisite: A.164/28A - - Additional for 422 (Session Interval Too Small) response

**Table A.216B: Supported header fields within the INVITE response**

| Item   | Header field | Sending |            |                | Receiving |            |                |
|--|--------------|---------|------------|----------------|-----------|------------|----------------|
|  |              | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1  | Min-SE       | [58] 5  | c1         | c1             | [58] 5    | c1         | c1             |
| c1: IF A.162/52 THEN m ELSE n/a - - the SIP session timer. |              |         |            |                |           |            |                |

**Table A.217: Void**

**Table A.217A: Void**

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/29H - - Additional for 470 (Consent Needed) response

**Table A.217AA: Supported header fields within the INVITE response**

| Item | Header field       | Sending        |            |                | Receiving      |            |                |
|------|--------------------|----------------|------------|----------------|----------------|------------|----------------|
|      |                    | Ref.           | RFC status | Profile status | Ref.           | RFC status | Profile status |
| 1    | Permission-Missing | [125]<br>5.9.3 | m          | m              | [125]<br>5.9.3 | m          | m              |

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/45 - - 503 (Service Unavailable)

**Table A.217B: Supported header fields within the INVITE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 8    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |



**Table A.217C: void**

|  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|
|  |  |  |  |  |  |  |  |
|--|--|--|--|--|--|--|--|

Prerequisite A.163/9 - - INVITE response

**Table A.218: Supported message bodies within the INVITE response**

| Item | Header   | Sending       |            |                | Receiving     |            |                |
|------|--|---------------|------------|----------------|---------------|------------|----------------|
|      |  | Ref.          | RFC status | Profile status | Ref.          | RFC status | Profile status |
| 1    | XML Schema for PSTN  | [11B]         |            | c1             | [11B]         |            | i              |
| 2    | Recipient List   | [183]         | c2         | c2             | [183]         | c3         | c3             |
| 3    | 3GPP IM CN subsystem XML body  | subclause 7.6 | n/a        | c4             | subclause 7.6 | n/a        | c5             |
| c1:  | A.3/3 OR A.3/4 OR A.3/5 OR A.3/7C OR A.3/9A OR A.3/10 OR A.3/11 OR A.3/13A THEN m ELSE n/a - - I-CSCF, S-CSCF, BGCF, AS acting as proxy, IBCF (THIG), additional routing functionality, E-CSCF, ISC gateway function (THIG). |               |            |                |               |            |                |
| c2:  | IF A.3/9B THEN m ELSE IF A.3/7A OR A.3/7B OR A.3/7D THEN m ELSE n/a - - IBCF (IMS-ALG), AS acting as terminating UA, AS acting as originating UA, AS performing 3 <sup>rd</sup> party call control.                          |               |            |                |               |            |                |
| c3:  | IF A.3/9B THEN m ELSE IF A.3/7A OR A.3/7B OR A.3/7D THEN i ELSE n/a - - IBCF (IMS-ALG), AS acting as terminating UA, AS acting as originating UA, AS performing 3 <sup>rd</sup> party call control.                          |               |            |                |               |            |                |
| c4:  | IF A.3/2 OR (A.3/9 AND NOT A.3/9B) OR A.3A/88 THEN m ELSE n/a - - P-CSCF, IBCF, IBCF (IMS-ALG), ATCF (proxy).  |               |            |                |               |            |                |
| c5:  | IF A.3/2 OR (A.3/9 AND NOT A.3/9B) OR A.3A/88 THEN i ELSE n/a - - P-CSCF, IBCF, IBCF (IMS-ALG), ATCF (proxy).  |               |            |                |               |            |                |

### A.2.2.4.7A MESSAGE method

Prerequisite A.163/9A - - MESSAGE request

**Table A.218A: Supported header fields within the MESSAGE request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept-Contact                | [56B] 9.2            | c28        | c28            | [56B] 9.2            | c28        | c29            |
| 1A   | Allow                         | [26] 20.5            | m          | m              | [50] 10              | i          | i              |
| 2    | Allow-Events                  | [28] 7.2.2           | m          | m              | [28] 7.2.2           | c1         | c1             |
| 3    | Authorization                 | [26] 20.7            | m          | m              | [26] 20.7            | i          | i              |
| 4    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 5    | Call-Info                     | [26] 20.9            | m          | m              | [26] 20.9            | c4         | c4             |
| 6    | Content-Disposition           | [26] 20.11           | m          | m              | [26] 20.11           | i          | i              |
| 7    | Content-Encoding              | [26] 20.12           | m          | m              | [26] 20.12           | i          | i              |
| 8    | Content-Language              | [26] 20.13           | m          | m              | [26] 20.13           | i          | i              |
| 9    | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 10   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | i          | i              |
| 11   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 12   | Date                          | [26] 20.17           | m          | m              | [26] 20.17           | c2         | c2             |
| 13   | Expires                       | [26] 20.19           | m          | m              | [26] 20.19           | l          | i              |
| 13A  | Feature-Caps                  | [190]                | c71        | c71            | [190]                | c71        | c71            |
| 14   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 14A  | Geolocation                   | [89] 4.1             | c36        | c36            | [89] 4.1             | c37        | c37            |
| 14B  | History-Info                  | [66] 4.1             | c32        | c32            | [66] 4.1             | c32        | c32            |
| 14C  | Geolocation-Routing           | [89] 4.1             | c36        | c36            | [89] 4.1             | c37        | c37            |
| 15   | In-Reply-To                   | [26] 20.21           | m          | m              | [50] 10              | i          | i              |
| 15A  | Max-Breadth                   | [117] 5.8            | c48        | c48            | [117] 5.8            | c49        | c49            |
| 16   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | m          | m              |
| 17   | MIME-Version                  | [26] 20.24           | m          | m              | [26] 20.24           | i          | i              |
| 18   | Organization                  | [26] 20.25           | m          | m              | [26] 20.25           | c3         | c3             |
| 18A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c23        | c23            | [52] 4.4,<br>[234] 2 | c24        | c24            |
| 18B  | P-Asserted-Identity           | [34] 9.1             | c10        | c10            | [34] 9.1             | c11        | c11            |
| 18C  | P-Asserted-Service            | [121] 4.1            | c40        | c40            | [121] 4.1            | c41        | c41            |
| 18D  | P-Called-Party-ID             | [52] 4.2             | c14        | c14            | [52] 4.2             | c15        | c16            |
| 18E  | P-Charging-Function-Addresses | [52] 4.5             | c21        | c21            | [52] 4.5             | c22        | c22            |
| 18F  | P-Charging-Vector             | [52] 4.6             | c19        | c19            | [52] 4.6             | c20        | c20            |
| 18H  | P-Preferred-Identity          | [34] 9.2             | x          | c69            | [34] 9.2             | c9         | c9             |
| 18I  | P-Preferred-Service           | [121] 4.2            | x          | x              | [121] 4.2            | c39        | c39            |
| 18J  | P-Private-Network-Indication  | [134]                | c44        | c44            | [134]                | c44        | c44            |
| 18K  | P-Profile-Key                 | [97] 5               | c34        | c34            | [97] 5               | c35        | c35            |
| 18L  | P-Served-User                 | [133] 6              | c45        | c45            | [133] 6              | c45        | c45            |
| 18M  | P-User-Database               | [82] 4               | c33        | c33            | [82] 4               | c33        | c33            |
| 18N  | P-Visited-Network-ID          | [52] 4.3             | c17        | n/a            | [52] 4.3             | c18        | n/a            |
| 19   | Priority                      | [26] 20.26           | m          | m              | [26] 20.26           | i          | i              |
| 19A  | Privacy                       | [33] 4.2             | c12        | c12            | [33] 4.2             | c13        | c13            |
| 20   | Proxy-Authorization           | [26] 20.28           | m          | m              | [26] 20.28           | c8         | c8             |
| 21   | Proxy-Require                 | [26] 20.29           | m          | m              | [26] 20.29           | m          | m              |
| 21A  | Reason                        | [34A] 2              | c26        | c26            | [34A] 2              | c27        | c27            |
| 22   | Record-Route                  | [26] 20.30           | m          | m              | [26] 20.30           | c7         | c7             |
| 22A  | Referred-By                   | [59] 3               | c30        | c30            | [59] 3               | c31        | c31            |
| 23   | Reject-Contact                | [56B] 9.2            | c28        | c28            | [56B] 9.2            | c28        | c29            |
| 23A  | Reply-To                      | [26] 20.31           | m          | m              | [26] 20.31           | i          | i              |
| 23B  | Request-Disposition           | [56B] 9.1            | c28        | c28            | [56B] 9.1            | c28        | c28            |
| 24   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | c5         | c5             |
| 24A  | Resource-Priority             | [116] 3.1            | c38        | c38            | [116] 3.1            | c38        | c38            |
| 25   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | m          | m              |
| 25A  | Security-Client               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c25        | c25            |
| 25B  | Security-Verify               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c25        | c25            |
| 26   | Subject                       | [26] 20.36           | m          | m              | [26] 20.36           | i          | i              |
| 25C  | Session-ID                    | [162]                | c70        | c70            | [162]                | c70        | c70            |
| 27   | Supported                     | [26] 20.37           | m          | m              | [26] 20.37           | c6         | c6             |
| 28   | Timestamp                     | [26] 20.38           | m          | m              | [26] 20.38           | i          | i              |
| 29   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 29A  | Trigger-Consent               | [125]<br>5.11.2      | c42        | c42            | [125]<br>5.11.2      | c43        | c43            |
| 30   | User-Agent                    | [26] 20.41           | m          | m              | [26] 20.41           | i          | i              |

| 31   | Via   | [26] 20.42 | m | m | [26] 20.42 | m | m |
|------|---|------------|---|---|------------|---|---|
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |            |   |   |            |   |   |
| c2:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |            |   |   |            |   |   |
| c3:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |            |   |   |            |   |   |
| c4:  | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |            |   |   |            |   |   |
| c5:  | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |            |   |   |            |   |   |
| c6:  | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.  |            |   |   |            |   |   |
| c7:  | IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.   |            |   |   |            |   |   |
| c8:  | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.  |            |   |   |            |   |   |
| c9:  | IF A.162/30A OR A.162/30C THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity, act as entity passing on identity transparently independent of trust domain.   |            |   |   |            |   |   |
| c10: | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |            |   |   |            |   |   |
| c11: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |            |   |   |            |   |   |
| c12: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |            |   |   |            |   |   |
| c13: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |            |   |   |            |   |   |
| c14: | IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension.   |            |   |   |            |   |   |
| c15: | IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension.   |            |   |   |            |   |   |
| c16: | IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND (A.3/3 OR A.3/9A) THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or (I-CSCF or IBCF (THIG)).   |            |   |   |            |   |   |
| c17: | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension.  |            |   |   |            |   |   |
| c18: | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response.   |            |   |   |            |   |   |
| c19: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |            |   |   |            |   |   |
| c20: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |            |   |   |            |   |   |
| c21: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |            |   |   |            |   |   |
| c22: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |            |   |   |            |   |   |
| c23: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |            |   |   |            |   |   |
| c24: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |            |   |   |            |   |   |
| c25: | IF A.162/47 OR A.162/47A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |            |   |   |            |   |   |
| c26: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |            |   |   |            |   |   |
| c27: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.  |            |   |   |            |   |   |
| c28: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |            |   |   |            |   |   |
| c29: | IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CSCF.   |            |   |   |            |   |   |
| c30: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.  |            |   |   |            |   |   |
| c31: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |            |   |   |            |   |   |
| c32: | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |            |   |   |            |   |   |
| c33: | IF A.162/60 THEN m ELSE n/a - - the P-User-Database private header extension.   |            |   |   |            |   |   |
| c34: | IF A.162/66A THEN m ELSE n/a - - making the first query to the database in order to populate the P-Profile-Key header.  |            |   |   |            |   |   |
| c35: | IF A.162/66B THEN m ELSE n/a - - using the information in the P-Profile-Key header.   |            |   |   |            |   |   |
| c36: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |            |   |   |            |   |   |
| c37: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |            |   |   |            |   |   |
| c38: | IF A.162/80A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.   |            |   |   |            |   |   |
| c39: | IF A.162/84A THEN m ELSE n/a - - act as authentication entity within the trust domain for asserted service.   |            |   |   |            |   |   |

|       |  |
|-------|--|
| c40:  | IF A.162/84 THEN m ELSE n/a - - SIP extension for the identification of services.  |
| c41:  | IF A.162/84 OR A.162/30B THEN m ELSE i - - SIP extension for the identification of services or subsequent entity within trust network that can route outside the trust network.                            |
| c42:  | IF A.162/85 THEN m ELSE n/a - - a framework for consent-based communications in SIP.   |
| c43:  | IF A.162/85 THEN i ELSE n/a - - a framework for consent-based communications in SIP.   |
| c44:  | IF A.162/87 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).  |
| c45:  | IF A.162/88 THEN m ELSE n/a - - the SIP P-Served-User private header.  |
| c49:  | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, forking of initial requests. |
| c69:  | IF A.162/30C THEN m ELSE x - - act as entity passing on identity transparently independent of trust domain.  |
| c70:  | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.  |
| c71:  | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.  |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.   |

Prerequisite A.163/9A - - MESSAGE request

**Table A.218B: Supported message bodies within the MESSAGE request**

| Item | Header  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | permission document   | [125] 5.4 | c1         | c1             | [125] 5.4 | c2         | c2             |
| 2    | application/vnd.3gpp.sms  | [4D]      | m          | m              | [4D]      | i          | i              |
| 2    | message/cpim  | [151]     | c3         | c3             | [151]     | c4         | c4             |
| 3    | message/imdn+xml  | [157]     | c5         | c5             | [157]     | c6         | c6             |
| c1:  | IF A.162/85 THEN m ELSE n/a - - a framework for consent-based communications in SIP.          |           |            |                |           |            |                |
| c2:  | IF A.162/85 THEN i ELSE n/a - - a framework for consent-based communications in SIP.          |           |            |                |           |            |                |
| c3:  | IF A.162/95 THEN m ELSE n/a - - common presence and instant messaging (CPIM): message format. |           |            |                |           |            |                |
| c4:  | IF A.162/95 THEN i ELSE n/a - - common presence and instant messaging (CPIM): message format. |           |            |                |           |            |                |
| c5:  | IF A.162/96 THEN m ELSE n/a - - instant message disposition notification.                     |           |            |                |           |            |                |
| c6:  | IF A.162/96 THEN i ELSE n/a - - instant message disposition notification.                     |           |            |                |           |            |                |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/1 - - Additional for 100 (Trying) response

**Table A.218BA: Supported header fields within the MESSAGE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID   | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length  | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq  | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date  | [26] 20.17 | c1         | c1             | [26] 20.17 | c2         | c2             |
| 5    | From  | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To  | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies. |            |            |                |            |            |                |
| c2:  | IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.   |            |            |                |            |            |                |

Prerequisite A.163/9B - - MESSAGE response for all remaining status-codes

**Table A.218C: Supported header fields within the MESSAGE response**

| Item | Header field                  | Sending                          |            |                | Receiving                        |            |                |
|------|-------------------------------|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |                               | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow                         | [26] 20.5                        | m          | m              | [26] 20.5                        | i          | i              |
| 1    | Call-ID                       | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 2    | Call-Info                     | [26] 20.9                        | m          | m              | [26] 20.9                        | c3         | c3             |
| 3    | Content-Disposition           | [26] 20.11                       | m          | m              | [26] 20.11                       | i          | i              |
| 4    | Content-Encoding              | [26] 20.12                       | m          | m              | [26] 20.12                       | i          | i              |
| 5    | Content-Language              | [26] 20.13                       | m          | m              | [26] 20.13                       | i          | i              |
| 6    | Content-Length                | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 7    | Content-Type                  | [26] 20.15                       | m          | m              | [26] 20.15                       | i          | i              |
| 8    | CSeq                          | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 9    | Date                          | [26] 20.17                       | m          | m              | [26] 20.17                       | c1         | c1             |
| 9A   | Expires                       | [26] 20.19                       | m          | m              | [26] 20.19                       | i          | i              |
| 10   | From                          | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 10A  | Geolocation-Error             | [89] 4.3                         | c17        | c17            | [89] 4.3                         | c18        | c18            |
| 10B  | History-Info                  | [66] 4.1                         | c16        | c16            | [66] 4.1                         | c16        | c16            |
| 11   | MIME-Version                  | [26] 20.24                       | m          | m              | [26] 20.24                       | i          | i              |
| 12   | Organization                  | [26] 20.25                       | m          | m              | [26] 20.25                       | c2         | c2             |
| 12A  | P-Access-Network-Info         | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c13        | c13            | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c14        | c14            |
| 12B  | P-Asserted-Identity           | [34] 9.1                         | c5         | c5             | [34] 9.1                         | c6         | c6             |
| 12C  | P-Charging-Function-Addresses | [52] 4.5,<br>[52A] 4             | c11        | c11            | [52] 4.5,<br>[52A] 4             | c12        | c12            |
| 12D  | P-Charging-Vector             | [52] 4.6,<br>[52A] 4             | c9         | n/a            | [52] 4.6,<br>[52A] 4             | c10        | n/a            |
| 12F  | P-Preferred-Identity          | [34] 9.2                         | x          | x              | [34] 9.2                         | c4         | n/a            |
| 12G  | Privacy                       | [33] 4.2                         | c7         | c7             | [33] 4.2                         | c8         | c8             |
| 12H  | Reply-To                      | [26] 20.31                       | m          | m              | [26] 20.31                       | i          | i              |
| 12I  | Require                       | [26] 20.32                       | m          | m              | [26] 20.32                       | c15        | c15            |
| 13   | Server                        | [26] 20.35                       | m          | m              | [26] 20.35                       | i          | i              |
| 13A  | Session-ID                    | [162]                            | c21        | c21            | [162]                            | c21        | c21            |
| 14   | Timestamp                     | [26] 20.38                       | i          | i              | [26] 20.38                       | i          | i              |
| 15   | To                            | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 16   | User-Agent                    | [26] 20.41                       | m          | m              | [26] 20.41                       | i          | i              |
| 17   | Via                           | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 18   | Warning                       | [26] 20.43                       | m          | m              | [26] 20.43                       | i          | i              |

|      |   |
|------|---|
| c1:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c2:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |
| c3:  | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |
| c4:  | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.   |
| c5:  | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c6:  | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |
| c7:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c8:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c9:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c10: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c11: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c12: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c13: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c14: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c15: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c16: | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c17: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c18: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c21: | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.218D: Supported header fields within the MESSAGE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Accept-Resource-Priority  | [116] 3.2  | c4         | c4             | [116] 3.2  | c4         | c4             |
| 1    | Allow-Events  | [28] 7.2.2 | m          | m              | [28] 7.2.2 | c1         | c1             |
| 2    | Authentication-Info   | [26] 20.6  | m          | m              | [26] 20.6  | i          | i              |
| 3    | Feature-Caps  | [190]      | c6         | c6             | [190]      | c6         | c6             |
| 4    | Record-Route  | [26] 20.30 | m          | m              | [26] 20.30 | c3         | c3             |
| 6    | Supported   | [26] 20.37 | m          | m              | [26] 20.37 | i          | i              |
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |            |            |                |            |            |                |
| c3:  | IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routing. |            |            |                |            |            |                |
| c4:  | IF A.162/80A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.     |            |            |                |            |            |                |
| c6:  | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.   |            |            |                |            |            |                |



Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.218DA: Supported header fields within the MESSAGE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | m          | m              | [26] 20.18 | i          | i              |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.218E: Supported header fields within the MESSAGE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | c1         | c1             |
| c1:  | IF A.162/19E THEN m ELSE i - - deleting Contact headers. |            |            |                |            |            |                |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.218F: Supported header fields within the MESSAGE response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 6    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.218G: Supported header fields within the MESSAGE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |

**Table A.218H: Void**

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.218I: Supported header fields within the MESSAGE response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 6    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type)

**Table A.218J: Supported header fields within the MESSAGE response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1 | m          | m              | [26] 20.1 | i          | i              |
| 2    | Accept-Encoding | [26] 20.2 | m          | m              | [26] 20.2 | i          | i              |
| 3    | Accept-Language | [26] 20.3 | m          | m              | [26] 20.3 | i          | i              |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.218JA: Supported header fields within the MESSAGE response**

| Item | Header field  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority  | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.162/80A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.218K: Supported header fields within the MESSAGE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | c3         | c3             |
| c3:  | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. |            |            |                |            |            |                |

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.218L: Supported header fields within the MESSAGE response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | c1         | c1             | [48] 2    | n/a        | n/a            |
| c1:  | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

**Table A.218M: Void**

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/29H - - Additional for 470 (Consent Needed) response

**Table A.218MA: Supported header fields within the MESSAGE response**

| Item | Header field       | Sending        |            |                | Receiving      |            |                |
|------|--------------------|----------------|------------|----------------|----------------|------------|----------------|
|      |                    | Ref.           | RFC status | Profile status | Ref.           | RFC status | Profile status |
| 1    | Permission-Missing | [125]<br>5.9.3 | m          | m              | [125]<br>5.9.3 | m          | m              |

Prerequisite A.163/9B - - MESSAGE response

**Table A.218N: Supported message bodies within the MESSAGE response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

## A.2.2.4.8 NOTIFY method

Prerequisite A.163/10 - - NOTIFY request

**Table A.219: Supported header fields within the NOTIFY request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | m          | m              | [26] 20.1            | i          | i              |
| 1A   | Accept-Contact                | [56B] 9.2            | c21        | c21            | [56B] 9.2            | c22        | c22            |
| 2    | Accept-Encoding               | [26] 20.2            | m          | m              | [26] 20.2            | i          | i              |
| 3    | Accept-Language               | [26] 20.3            | m          | m              | [26] 20.3            | i          | i              |
| 3A   | Allow                         | [26] 20.5            | m          | m              | [26] 20.5            | i          | i              |
| 4    | Allow-Events                  | [28] 7.2.2           | m          | m              | [28] 7.2.2           | c1         | c1             |
| 5    | Authorization                 | [26] 20.7            | m          | m              | [26] 20.7            | i          | i              |
| 6    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 6A   | Call-Info                     | [26] 20.9            | m          | m              | [26] 20.9            | c28        | c28            |
| 6B   | Contact                       | [26] 20.10           | m          | m              | [26] 20.10           | i          | i              |
| 7    | Content-Disposition           | [26] 20.11           | m          | m              | [26] 20.11           | i          | i              |
| 8    | Content-Encoding              | [26] 20.12           | m          | m              | [26] 20.12           | i          | i              |
| 9    | Content-Language              | [26] 20.13           | m          | m              | [26] 20.13           | i          | i              |
| 10   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 11   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | i          | i              |
| 12   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 13   | Date                          | [26] 20.17           | m          | m              | [26] 20.17           | c2         | c2             |
| 14   | Event                         | [28] 7.2.1           | m          | m              | [28] 7.2.1           | m          | m              |
| 14A  | Feature-Caps                  | [190]                | c41        | c41            | [190]                | c41        | c41            |
| 15   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 15A  | Geolocation                   | [89] 4.1             | c26        | c26            | [89] 4.1             | c27        | c27            |
| 15B  | Geolocation-Routing           | [89] 4.1             | c26        | c26            | [89] 4.1             | c27        | c27            |
| 15C  | History-Info                  | [66] 4.1             | c25        | c25            | [66] 4.1             | c25        | c25            |
| 15D  | Max-Breadth                   | [117] 5.8            | c29        | c29            | [117] 5.8            | c30        | c30            |
| 16   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | m          | m              |
| 17   | MIME-Version                  | [26] 20.24           | m          | m              | [26] 20.24           | i          | i              |
| 17A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c16        | c16            | [52] 4.4,<br>[234] 2 | c17        | c17            |
| 17B  | P-Asserted-Identity           | [34] 9.1             | c8         | c8             | [34] 9.1             | c9         | c9             |
| 17C  | P-Charging-Function-Addresses | [52] 4.5             | c14        | c14            | [52] 4.5             | c15        | c15            |
| 17D  | P-Charging-Vector             | [52] 4.6             | c12        | n/a            | [52] 4.6             | c13        | n/a            |
| 17F  | P-Preferred-Identity          | [34] 9.2             | x          | x              | [34] 9.2             | c3         | n/a            |
| 17G  | Privacy                       | [33] 4.2             | c10        | c10            | [33] 4.2             | c11        | c11            |
| 18   | Proxy-Authorization           | [26] 20.28           | m          | m              | [26] 20.28           | c4         | c4             |
| 19   | Proxy-Require                 | [26] 20.29           | m          | m              | [26] 20.29           | m          | m              |
| 19A  | Reason                        | [34A] 2              | c19        | c19            | [34A] 2              | c20        | c20            |
| 20   | Record-Route                  | [26] 20.30           | m          | m              | [26] 20.30           | c7         | c7             |
| 20A  | Referred-By                   | [59] 3               | c23        | c23            | [59] 3               | c24        | c24            |
| 20B  | Reject-Contact                | [56B] 9.2            | c21        | c21            | [56B] 9.2            | c22        | c22            |
| 20C  | Request-Disposition           | [56B] 9.1            | c21        | c21            | [56B] 9.1            | c22        | c22            |
| 21   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | c5         | c5             |
| 22   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | m          | m              |
| 22A  | Security-Client               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c18        | c18            |
| 22B  | Security-Verify               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c18        | c18            |
| 22C  | Session-ID                    | [162]                | c40        | c40            | [162]                | c40        | c40            |
| 23   | Subscription-State            | [28] 8.2.3           | m          | m              | [28] 8.2.3           | i          | i              |
| 24   | Supported                     | [26] 20.37           | m          | m              | [26] 20.37           | c6         | c6             |
| 24A  | Resource-Priority             | [116] 3.1            | c36        | c36            | [116] 3.1            | c36        | c36            |
| 25   | Timestamp                     | [26] 20.38           | m          | m              | [26] 20.38           | i          | i              |
| 26   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 27   | User-Agent                    | [26] 20.41           | m          | m              | [26] 20.41           | i          | i              |
| 28   | Via                           | [26] 20.42           | m          | m              | [26] 20.42           | m          | m              |
| 29   | Warning                       | [26] 20.43           | m          | m              | [26] 20.43           | i          | i              |

|       |   |
|-------|---|
| c1:   | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |
| c2:   | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c3:   | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.   |
| c4:   | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.  |
| c5:   | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6:   | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.  |
| c7:   | IF A.162/14 THEN (IF A.162/22 OR A.162/27 THEN m ELSE o) ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog or (the REFER method or SIP specific event notification).  |
| c8:   | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c9:   | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |
| c10:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c11:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c12:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c13:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c14:  | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c15:  | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c16:  | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c17:  | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c18:  | IF A.162/47 OR A.162/47A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |
| c19:  | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c20:  | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c21:  | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c22:  | IF A.162/50 THEN i ELSE n/a - - caller preferences for the session initiation protocol.   |
| c23:  | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.  |
| c24:  | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c25:  | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c26:  | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c27:  | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c28:  | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |
| c29:  | IF A.162/81 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |
| c30:  | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, forking of initial requests.  |
| c36:  | IF A.162/80A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.   |
| c40:  | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |
| c41:  | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.   |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.  |

Prerequisite A.163/10 - - NOTIFY request

**Table A.220: Supported message bodies within the NOTIFY request**

| Item | Header        | Sending |            |                | Receiving |            |                |
|------|---------------|---------|------------|----------------|-----------|------------|----------------|
|      |               | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | sipfrag       | [37] 2  | m          | m              | [37] 2    | i          | i              |
| 2    | event package | [28]    | m          | m              | [28]      | i          | i              |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/1 - - Additional for 100 (Trying) response

**Table A.220A: Supported header fields within the NOTIFY response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID   | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length  | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq  | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date  | [26] 20.17 | c1         | c1             | [26] 20.17 | c2         | c2             |
| 5    | From  | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To  | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies. |            |            |                |            |            |                |
| c2:  | IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.   |            |            |                |            |            |                |

Prerequisite A.163/11 - - NOTIFY response for all remaining status-codes

**Table A.221: Supported header fields within the NOTIFY response**



| Item | Header field  | Sending                          |            |                | Receiving                        |            |                |
|------|---|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |   | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow   | [26] 20.5                        | m          | m              | [26] 20.5                        | i          | i              |
| 1    | Call-ID   | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 2    | Content-Disposition   | [26] 20.11                       | m          | m              | [26] 20.11                       | i          | i              |
| 3    | Content-Encoding  | [26] 20.12                       | m          | m              | [26] 20.12                       | i          | i              |
| 4    | Content-Language  | [26] 20.13                       | m          | m              | [26] 20.13                       | i          | i              |
| 5    | Content-Length  | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6    | Content-Type  | [26] 20.15                       | m          | m              | [26] 20.15                       | i          | i              |
| 7    | CSeq  | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8    | Date  | [26] 20.17                       | m          | m              | [26] 20.17                       | c1         | c1             |
| 9    | From  | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A   | Geolocation-Error   | [89] 4.3                         | c14        | c14            | [89] 4.3                         | c15        | c15            |
| 10   | MIME-Version  | [26] 20.24                       | m          | m              | [26] 20.24                       | i          | i              |
| 10A  | P-Access-Network-Info   | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c11        | c11            | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c12        | c12            |
| 10B  | P-Asserted-Identity   | [34] 9.1                         | c3         | c3             | [34] 9.1                         | c4         | c4             |
| 10C  | P-Charging-Function-Addresses   | [52] 4.5,<br>[52A] 4             | c9         | c9             | [52] 4.5,<br>[52A] 4             | c10        | c10            |
| 10D  | P-Charging-Vector   | [52] 4.6,<br>[52A] 4             | c7         | n/a            | [52] 4.6,<br>[52A] 4             | c8         | n/a            |
| 10F  | P-Preferred-Identity  | [34] 9.2                         | x          | x              | [34] 9.2                         | c2         | n/a            |
| 10G  | Privacy   | [33] 4.2                         | c5         | c5             | [33] 4.2                         | c6         | c6             |
| 10H  | Require   | [26] 20.32                       | m          | m              | [26] 20.32                       | c13        | c13            |
| 10I  | Server  | [26] 20.35                       | m          | m              | [26] 20.35                       | i          | i              |
| 10J  | Session-ID  | [162]                            | c18        | c18            | [162]                            | c18        | c18            |
| 11   | Timestamp   | [26] 20.38                       | m          | m              | [26] 20.38                       | i          | i              |
| 12   | To  | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 12A  | User-Agent  | [26] 20.41                       | m          | m              | [26] 20.41                       | i          | i              |
| 13   | Via   | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 14   | Warning   | [26] 20.43                       | m          | m              | [26] 20.43                       | i          | i              |
| c1:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c2:  | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.   |                                  |            |                |                                  |            |                |
| c3:  | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |                                  |            |                |                                  |            |                |
| c4:  | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |                                  |            |                |                                  |            |                |
| c5:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |                                  |            |                |                                  |            |                |
| c6:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |                                  |            |                |                                  |            |                |
| c7:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |                                  |            |                |                                  |            |                |
| c8:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c9:  | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |                                  |            |                |                                  |            |                |
| c10: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |                                  |            |                |                                  |            |                |
| c11: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |                                  |            |                |                                  |            |                |
| c12: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |                                  |            |                |                                  |            |                |
| c13: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |                                  |            |                |                                  |            |                |
| c14: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |                                  |            |                |                                  |            |                |
| c15: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |                                  |            |                |                                  |            |                |
| c18: | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.222: Supported header fields within the NOTIFY response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Accept-Resource-Priority   | [116] 3.2  | c4         | c4             | [116] 3.2  | c4         | c4             |
| 0B   | Allow-Events   | [28] 7.2.2 | m          | m              | [28] 7.2.2 | c1         | c1             |
| 1    | Authentication-Info  | [26] 20.6  | m          | m              | [26] 20.6  | i          | i              |
| 1A   | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | i          | i              |
| 1B   | Feature-Caps   | [190]      | c6         | c6             | [190]      | c6         | c6             |
| 2    | Record-Route   | [26] 20.30 | m          | m              | [26] 20.30 | c3         | c3             |
| 5    | Supported  | [26] 20.37 | m          | m              | [26] 20.37 | i          | i              |
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.   |            |            |                |            |            |                |
| c3:  | IF A.162/15 THEN m ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing. |            |            |                |            |            |                |
| c4:  | IF A.162/80A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.      |            |            |                |            |            |                |
| c6:  | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.  |            |            |                |            |            |                |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.222A: Supported header fields within the NOTIFY response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | m          | m              | [26] 20.18 | i          | i              |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/103 - - Additional for 3xx response

**Table A.223: Supported header fields within the NOTIFY response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | c1         | c1             |
| c1:  | IF A.162/19E THEN m ELSE i - - deleting Contact headers. |            |            |                |            |            |                |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.224: Supported header fields within the NOTIFY response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 8    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.225: Supported header fields within the NOTIFY response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |

**Table A.226: Void**

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.227: Supported header fields within the NOTIFY response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 6    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.228: Supported header fields within the NOTIFY response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1 | m          | m              | [26] 20.1 | i          | i              |
| 2    | Accept-Encoding | [26] 20.2 | m          | m              | [26] 20.2 | i          | i              |
| 3    | Accept-Language | [26] 20.3 | m          | m              | [26] 20.3 | i          | i              |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.228A: Supported header fields within the NOTIFY response**

| Item | Header field  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority  | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.162/80A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.229: Supported header fields within the NOTIFY response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | c3         | c3             |
| c3:  | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. |            |            |                |            |            |                |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.229A: Supported header fields within the NOTIFY response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | c1         | c1             | [48] 2    | n/a        | n/a            |
| c1:  | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

**Table A.230: Void**

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/35 - - Additional for 485 (Ambiguous) response

**Table A.230A: Supported header fields within the NOTIFY response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Contact      | [26] 20.10 | m          | m              | [26] 20.10 | i          | i              |

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/39 - - Additional for 489 (Bad Event) response

**Table A.231: Supported header fields within the NOTIFY response**

| Item   | Header field | Sending    |            |                | Receiving  |            |                |
|--|--------------|------------|------------|----------------|------------|------------|----------------|
|  |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1  | Allow-Events | [28] 7.2.2 | m          | m              | [28] 7.2.2 | c1         | c1             |
| c1: IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.   |              |            |            |                |            |            |                |
| NOTE: c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. |              |            |            |                |            |            |                |

Prerequisite A.163/11 - - NOTIFY response

**Table A.232: Supported message bodies within the NOTIFY response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

#### A.2.2.4.9 OPTIONS method

Prerequisite A.163/12 - - OPTIONS request

**Table A.233: Supported header fields within the OPTIONS request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | m          | m              | [26] 20.1            | i          | i              |
| 1A   | Accept-Contact                | [56B] 9.2            | c28        | c28            | [56B] 9.2            | c28        | c29            |
| 2    | Accept-Encoding               | [26] 20.2            | m          | m              | [26] 20.2            | i          | i              |
| 3    | Accept-Language               | [26] 20.3            | m          | m              | [26] 20.3            | i          | i              |
| 3A   | Allow                         | [26] 20.5            | m          | m              | [26] 20.5            | i          | i              |
| 4    | Allow-Events                  | [28] 7.2.2           | m          | m              | [28] 7.2.2           | c1         | c1             |
| 5    | Authorization                 | [26] 20.7            | m          | m              | [26] 20.7            | i          | i              |
| 6    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 7    | Call-Info                     | [26] 20.9            | m          | m              | [26] 20.9            | c4         | c4             |
| 8    | Contact                       | [26] 20.10           | m          | m              | [26] 20.10           | i          | i              |
| 9    | Content-Disposition           | [26] 20.11           | m          | m              | [26] 20.11           | i          | i              |
| 10   | Content-Encoding              | [26] 20.12           | m          | m              | [26] 20.12           | i          | i              |
| 11   | Content-Language              | [26] 20.13           | m          | m              | [26] 20.13           | i          | i              |
| 12   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 13   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | i          | i              |
| 14   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 15   | Date                          | [26] 20.17           | m          | m              | [26] 20.17           | c2         | c2             |
| 15A  | Feature-Caps                  | [190]                | c57        | c57            | [190]                | c57        | c57            |
| 16   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 16A  | Geolocation                   | [89] 4.1             | c36        | c36            | [89] 4.1             | c37        | c37            |
| 16B  | Geolocation-Routing           | [89] 4.1             | c36        | c36            | [89] 4.1             | c37        | c37            |
| 16C  | History-Info                  | [66] 4.1             | c32        | c32            | [66] 4.1             | c32        | c32            |
| 16D  | Max-Breadth                   | [117] 5.8            | c41        | c41            | [117] 5.8            | c42        | c42            |
| 17   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | m          | m              |
| 18   | MIME-Version                  | [26] 20.24           | m          | m              | [26] 20.24           | i          | i              |
| 19   | Organization                  | [26] 20.25           | m          | m              | [26] 20.25           | c3         | c3             |
| 19A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c23        | c23            | [52] 4.4,<br>[234] 2 | c24        | c24            |
| 19B  | P-Asserted-Identity           | [34] 9.1             | c10        | c10            | [34] 9.1             | c11        | c11            |
| 19C  | P-Asserted-Service            | [121] 4.1            | c39        | c39            | [121] 4.1            | c40        | c40            |
| 19D  | P-Called-Party-ID             | [52] 4.2             | c14        | c14            | [52] 4.2             | c15        | c16            |
| 19E  | P-Charging-Function-Addresses | [52] 4.5             | c21        | c21            | [52] 4.5             | c22        | c22            |
| 19F  | P-Charging-Vector             | [52] 4.6             | c19        | c19            | [52] 4.6             | c20        | c20            |
| 19H  | P-Preferred-Identity          | [34] 9.2             | x          | c54            | [34] 9.2             | c9         | c55            |
| 19I  | P-Preferred-Service           | [121] 4.2            | x          | x              | [121] 4.2            | c38        | c38            |
| 19J  | P-Private-Network-Indication  | [134]                | c48        | c48            | [134]                | c48        | c48            |
| 19K  | P-Profile-Key                 | [97] 5               | c34        | c34            | [97] 5               | c35        | c35            |
| 19L  | P-Served-User                 | [133] 6              | c49        | c49            | [133] 6              | c49        | c49            |
| 19M  | P-User-Database               | [82] 4               | c33        | c33            | [82] 4               | c33        | c33            |
| 19N  | P-Visited-Network-ID          | [52] 4.3             | c17        | n/a            | [52] 4.3             | c18        | n/a            |
| 19O  | Privacy                       | [33] 4.2             | c12        | c12            | [33] 4.2             | c13        | c13            |
| 20   | Proxy-Authorization           | [26] 20.28           | m          | m              | [26] 20.28           | c8         | c8             |
| 21   | Proxy-Require                 | [26] 20.29           | m          | m              | [26] 20.29           | m          | m              |
| 21A  | Reason                        | [34A] 2              | c26        | c26            | [34A] 2              | c27        | c27            |
| 22   | Record-Route                  | [26] 20.30           | m          | m              | [26] 20.30           | c7         | c7             |
| 22A  | Recv-Info                     | [25] 5.2.3           | c52        | c52            | [25] 5.2.3           | c53        | c53            |
| 22B  | Referred-By                   | [59] 3               | c30        | c30            | [59] 3               | c31        | c31            |
| 22C  | Reject-Contact                | [56B] 9.2            | c28        | c28            | [56B] 9.2            | c28        | c29            |
| 22D  | Request-Disposition           | [56B] 9.1            | c28        | c28            | [56B] 9.1            | c28        | c28            |
| 23   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | c5         | c5             |
| 23A  | Resource-Priority             | [116] 3.1            | c47        | c47            | [116] 3.1            | c47        | c47            |
| 24   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | m          | m              |
| 24A  | Security-Client               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c25        | c25            |
| 24B  | Security-Verify               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c25        | c25            |
| 24C  | Session-ID                    | [162]                | c56        | c56            | [162]                | c56        | c56            |
| 25   | Supported                     | [26] 20.37           | m          | m              | [26] 20.37           | c6         | c6             |
| 26   | Timestamp                     | [26] 20.38           | m          | m              | [26] 20.38           | i          | i              |
| 27   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 28   | User-Agent                    | [26] 20.41           | m          | m              | [26] 20.41           | i          | i              |
| 29   | Via                           | [26] 20.42           | m          | m              | [26] 20.42           | m          | m              |

|      |   |
|------|---|
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |
| c2:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c3:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |
| c4:  | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |
| c5:  | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6:  | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.  |
| c7:  | IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.   |
| c8:  | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.  |
| c9:  | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.   |
| c10: | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c11: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |
| c12: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c13: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c14: | IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension.   |
| c15: | IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension.   |
| c16: | IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND (A.3/3 OR A.3/9A) THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or (I-CSCF or IBCF (THIG)).   |
| c17: | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension.  |
| c18: | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response.   |
| c19: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c20: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c21: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c22: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c23: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c24: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c25: | IF A.162/47 OR A.162/47A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |
| c26: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c27: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c28: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c29: | IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CSCF.   |
| c30: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.  |
| c31: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c32: | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c33: | IF A.162/60 THEN m ELSE n/a - - the P-User-Database private header extension.   |
| c34: | IF A.162/66A THEN m ELSE n/a - - making the first query to the database in order to populate the P-Profile-Key header.  |
| c35: | IF A.162/66B THEN m ELSE n/a - - using the information in the P-Profile-Key header.   |
| c36: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c37: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c38: | IF A.162/84A THEN m ELSE n/a - - act as authentication entity within the trust domain for asserted service.   |
| c39: | IF A.162/84 THEN m ELSE n/a - - SIP extension for the identification of services.   |
| c40: | IF A.162/84 OR A.162/30B THEN m ELSE i - - SIP extension for the identification of services or subsequent entity within trust network that can route outside the trust network.   |
| c41: | IF A.162/81 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |



|       |  |
|-------|--|
| c42:  | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, forking of initial requests. |
| c47:  | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.  |
| c48:  | IF A.162/87 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).  |
| c49:  | IF A.162/88 THEN m ELSE n/a - - the SIP P-Served-User private header.  |
| c52:  | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.   |
| c53:  | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.   |
| c54:  | IF A.162/30C THEN m ELSE x - - act as entity passing on identity transparently independent of trust domain.  |
| c55:  | IF A.162/30A OR A.162/30C THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity, act as entity passing on identity transparently independent of trust domain.              |
| c56:  | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.  |
| c57:  | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.  |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.   |

Prerequisite A.163/12 - - OPTIONS request

**Table A.234: Supported message bodies within the OPTIONS request**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

**Table A.235: Void**

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/1 - - Additional for 100 (Trying) response

**Table A.235A: Supported header fields within the OPTIONS response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID   | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length  | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq  | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date  | [26] 20.17 | c1         | c1             | [26] 20.17 | c2         | c2             |
| 5    | From  | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To  | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies. |            |            |                |            |            |                |
| c2:  | IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.   |            |            |                |            |            |                |

Prerequisite A.163/13 - - OPTIONS response for all remaining status-codes

**Table A.236: Supported header fields within the OPTIONS response**

| Item | Header field                  | Sending                          |            |                | Receiving                        |            |                |
|------|-------------------------------|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |                               | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow                         | [26] 20.5                        | m          | m              | [26] 20.5                        | i          | i              |
| 1    | Call-ID                       | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 1A   | Call-Info                     | [26] 20.9                        | m          | m              | [26] 20.9                        | c3         | c3             |
| 2    | Content-Disposition           | [26] 20.11                       | m          | m              | [26] 20.11                       | i          | i              |
| 3    | Content-Encoding              | [26] 20.12                       | m          | m              | [26] 20.12                       | i          | i              |
| 4    | Content-Language              | [26] 20.13                       | m          | m              | [26] 20.13                       | i          | i              |
| 5    | Content-Length                | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6    | Content-Type                  | [26] 20.15                       | m          | m              | [26] 20.15                       | i          | i              |
| 7    | CSeq                          | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8    | Date                          | [26] 20.17                       | m          | m              | [26] 20.17                       | c1         | c1             |
| 9    | From                          | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A   | Geolocation-Error             | [89] 4.3                         | c17        | c17            | [89] 4.3                         | c18        | c18            |
| 9B   | History-Info                  | [66] 4.1                         | c16        | c16            | [66] 4.1                         | c16        | c16            |
| 10   | MIME-Version                  | [26] 20.24                       | m          | m              | [26] 20.24                       | i          | i              |
| 11   | Organization                  | [26] 20.25                       | m          | m              | [26] 20.25                       | c2         | c2             |
| 11A  | P-Access-Network-Info         | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c13        | c13            | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c14        | c14            |
| 11B  | P-Asserted-Identity           | [34] 9.1                         | c5         | c5             | [34] 9.1                         | c6         | c6             |
| 11C  | P-Charging-Function-Addresses | [52] 4.5,<br>[52A] 4             | c11        | c11            | [52] 4.5,<br>[52A] 4             | c12        | c12            |
| 11D  | P-Charging-Vector             | [52] 4.6,<br>[52A] 4             | c9         | c9             | [52] 4.6,<br>[52A] 4             | c10        | c10            |
| 11F  | P-Preferred-Identity          | [34] 9.2                         | x          | x              | [34] 9.2                         | c4         | n/a            |
| 11G  | Privacy                       | [33] 4.2                         | c7         | c7             | [33] 4.2                         | c8         | c8             |
| 11H  | Recv-Info                     | [25] 5.2.3                       | c21        | c21            | [25] 5.2.3                       | c22        | c22            |
| 11I  | Require                       | [26] 20.32                       | m          | m              | [26] 20.32                       | c15        | c15            |
| 11J  | Server                        | [26] 20.35                       | m          | m              | [26] 20.35                       | i          | i              |
| 11K  | Session-ID                    | [162]                            | c23        | c23            | [162]                            | c23        | c23            |
| 12   | Timestamp                     | [26] 20.38                       | m          | m              | [26] 20.38                       | i          | i              |
| 13   | To                            | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 13A  | User-Agent                    | [26] 20.41                       | m          | m              | [26] 20.41                       | i          | i              |
| 14   | Via                           | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 15   | Warning                       | [26] 20.43                       | m          | m              | [26] 20.43                       | i          | i              |

|      |   |
|------|---|
| c1:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c2:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |
| c3:  | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |
| c4:  | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.   |
| c5:  | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c6:  | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |
| c7:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c8:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c9:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c10: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c11: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c12: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c13: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c14: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c15: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c16: | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c17: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c18: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c21: | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |
| c22: | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |
| c23: | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.237: Supported header fields within the OPTIONS response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Accept  | [26] 20.1  | m          | m              | [26] 20.1  | i          | i              |
| 1A   | Accept-Encoding   | [26] 20.2  | m          | m              | [26] 20.2  | i          | i              |
| 1B   | Accept-Language   | [26] 20.3  | m          | m              | [26] 20.3  | i          | i              |
| 1C   | Accept-Resource-Priority  | [116] 3.2  | c12        | c12            | [116] 3.2  | c12        | c12            |
| 2    | Allow-Events  | [28] 7.2.2 | m          | m              | [28] 7.2.2 | c1         | c1             |
| 3    | Authentication-Info   | [26] 20.6  | m          | m              | [26] 20.6  | i          | i              |
| 5    | Contact   | [26] 20.10 | m          | m              | [26] 20.10 | i          | i              |
| 6    | Feature-Caps  | [190]      | c14        | c14            | [190]      | c14        | c14            |
| 7    | Recv-Info   | [25] 5.2.3 | c7         | c7             | [25] 5.2.3 | c8         | c8             |
| 9    | Record-Route  | [26] 20.30 | m          | m              | [26] 20.30 | c3         | c3             |
| 12   | Supported   | [26] 20.37 | m          | m              | [26] 20.37 | i          | i              |
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |            |            |                |            |            |                |
| c3:  | IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routing. |            |            |                |            |            |                |
| c7:  | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |            |            |                |            |            |                |
| c8:  | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |            |            |                |            |            |                |
| c12: | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.   |            |            |                |            |            |                |
| c14: | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.   |            |            |                |            |            |                |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.237A: Supported header fields within the OPTIONS response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | m          | m              | [26] 20.18 | i          | i              |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.238: Supported header fields within the OPTIONS response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | c1         | c1             |
| c1:  | IF A.162/19E THEN m ELSE i - - deleting Contact headers. |            |            |                |            |            |                |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.239: Supported header fields within the OPTIONS response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 10   | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.240: Supported header fields within the OPTIONS response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |

**Table A.241: Void**

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.242: Supported header fields within the OPTIONS response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 8    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.243: Supported header fields within the OPTIONS response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1 | m          | m              | [26] 20.1 | i          | i              |
| 2    | Accept-Encoding | [26] 20.2 | m          | m              | [26] 20.2 | i          | i              |
| 3    | Accept-Language | [26] 20.3 | m          | m              | [26] 20.3 | i          | i              |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.243A: Supported header fields within the OPTIONS response**

| Item  | Header field             | Sending   |            |                | Receiving |            |                |
|---|--------------------------|-----------|------------|----------------|-----------|------------|----------------|
|   |                          | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1   | Accept-Resource-Priority | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1: IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol. |                          |           |            |                |           |            |                |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.244: Supported header fields within the OPTIONS response**

| Item   | Header field | Sending    |            |                | Receiving  |            |                |
|--|--------------|------------|------------|----------------|------------|------------|----------------|
|  |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 7  | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | c3         | c3             |
| c3: IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. |              |            |            |                |            |            |                |

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.244A: Supported header fields within the OPTIONS response**

| Item  | Header field    | Sending |            |                | Receiving |            |                |
|---|-----------------|---------|------------|----------------|-----------|------------|----------------|
|   |                 | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3   | Security-Server | [48] 2  | c1         | c1             | [48] 2    | n/a        | n/a            |
| c1: IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |                 |         |            |                |           |            |                |

**Table A.245: Void**

Prerequisite A.163/13 - - OPTIONS response

**Table A.246: Supported message bodies within the OPTIONS response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

#### A.2.2.4.10 PRACK method

Prerequisite A.163/14 - - PRACK request

**Table A.247: Supported header fields within the PRACK request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | m          | m              | [26] 20.1            | i          | i              |
| 1A   | Accept-Contact                | [56B] 9.2            | c18        | c18            | [56B] 9.2            | c19        | c19            |
| 2    | Accept-Encoding               | [26] 20.2            | m          | m              | [26] 20.2            | i          | i              |
| 3    | Accept-Language               | [26] 20.3            | m          | m              | [26] 20.3            | i          | i              |
| 3A   | Allow                         | [26] 20.5            | m          | m              | [26] 20.5            | i          | i              |
| 4    | Allow-Events                  | [28] 7.2.2           | m          | m              | [28] 7.2.2           | c1         | c1             |
| 5    | Authorization                 | [26] 20.7            | m          | m              | [26] 20.7            | i          | i              |
| 6    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 7    | Content-Disposition           | [26] 20.11           | m          | m              | [26] 20.11           | i          | c3             |
| 8    | Content-Encoding              | [26] 20.12           | m          | m              | [26] 20.12           | i          | c3             |
| 9    | Content-Language              | [26] 20.13           | m          | m              | [26] 20.13           | i          | c3             |
| 10   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 11   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | i          | c3             |
| 12   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 13   | Date                          | [26] 20.17           | m          | m              | [26] 20.17           | c2         | c2             |
| 14   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 14A  | Max-Breadth                   | [117] 5.8            | c26        | c26            | [117] 5.8            | c27        | c27            |
| 15   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | m          | m              |
| 16   | MIME-Version                  | [26] 20.24           | m          | m              | [26] 20.24           | i          | c3             |
| 16A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c14        | c14            | [52] 4.4,<br>[234] 2 | c15        | c15            |
| 16B  | P-Charging-Function-Addresses | [52] 4.5             | c12        | c12            | [52] 4.5             | c13        | c13            |
| 16C  | P-Charging-Vector             | [52] 4.6             | c10        | n/a            | [52] 4.6             | c11        | n/a            |
| 16E  | P-Early-Media                 | [109] 8              | o          | c22            | [109] 8              | o          | c23            |
| 16F  | Privacy                       | [33] 4.2             | c8         | c8             | [33] 4.2             | c9         | c9             |
| 17   | Proxy-Authorization           | [26] 20.28           | m          | m              | [26] 20.28           | c4         | c4             |
| 18   | Proxy-Require                 | [26] 20.29           | m          | m              | [26] 20.29           | m          | m              |
| 19   | RAck                          | [27] 7.2             | m          | m              | [27] 7.2             | i          | i              |
| 19A  | Reason                        | [34A] 2              | c16        | c16            | [34A] 2              | c17        | c17            |
| 20   | Record-Route                  | [26] 20.30           | m          | m              | [26] 20.30           | c7         | c7             |
| 20A  | Recv-Info                     | [25] 5.2.3           | c28        | c28            | [25] 5.2.3           | c29        | c29            |
| 20B  | Referred-By                   | [59] 3               | c20        | c20            | [59] 3               | c21        | c21            |
| 20C  | Reject-Contact                | [56B] 9.2            | c18        | c18            | [56B] 9.2            | c19        | c19            |
| 20D  | Request-Disposition           | [56B] 9.1            | c18        | c18            | [56B] 9.1            | c19        | c19            |
| 21   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | c5         | c5             |
| 21A  | Resource-Priority             | [16] 3.1             | c47        | c47            | [116] 3.1            | c47        | c47            |
| 22   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | m          | m              |
| 22A  | Session-ID                    | [162]                | c48        | c48            | [162]                | c48        | c48            |
| 23   | Supported                     | [26] 20.37           | m          | m              | [26] 20.37           | c6         | c6             |
| 24   | Timestamp                     | [26] 20.38           | m          | m              | [26] 20.38           | i          | i              |
| 25   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 26   | User-Agent                    | [26] 20.41           | m          | m              | [26] 20.41           | i          | i              |
| 27   | Via                           | [26] 20.42           | m          | m              | [26] 20.42           | m          | m              |



|       |   |
|-------|---|
| c1:   | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |
| c2:   | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c3:   | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.   |
| c4:   | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.  |
| c5:   | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6:   | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.  |
| c7:   | IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.   |
| c8:   | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c9:   | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c10:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c11:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c12:  | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c13:  | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c14:  | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c15:  | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c16:  | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c17:  | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c18:  | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c19:  | IF A.162/50 THEN i ELSE n/a - - caller preferences for the session initiation protocol.   |
| c20:  | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.  |
| c21:  | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c22:  | IF A.162/76 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.  |
| c23:  | IF A.162/76 THEN (IF A.3/2 THEN m ELSE i) ELSE n/a - - P-CSCF, using the information in the P-Early-Media header.   |
| c26:  | IF A.162/81 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |
| c27:  | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, forking of initial requests.  |
| c28:  | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |
| c29:  | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |
| c47:  | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.   |
| c48:  | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.  |

Prerequisite A.163/14 - - PRACK request

**Table A.248: Supported message bodies within the PRACK request**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

**Table A.249: Void**

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/1 - - Additional for 100 (Trying) response

**Table A.249A: Supported header fields within the PRACK response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID   | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length  | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq  | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date  | [26] 20.17 | c1         | c1             | [26] 20.17 | c2         | c2             |
| 5    | From  | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To  | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies. |            |            |                |            |            |                |
| c2:  | IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.   |            |            |                |            |            |                |

Prerequisite A.163/15 - - PRACK response for all remaining status-codes

**Table A.250: Supported header fields within the PRACK response**

| Item | Header field  | Sending                          |            |                | Receiving                        |            |                |
|------|---|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |   | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow   | [26] 20.5                        | m          | m              | [26] 20.5                        | i          | i              |
| 1    | Call-ID   | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 2    | Content-Disposition   | [26] 20.11                       | m          | m              | [26] 20.11                       | i          | c2             |
| 3    | Content-Encoding  | [26] 20.12                       | m          | m              | [26] 20.12                       | i          | c2             |
| 4    | Content-Language  | [26] 20.13                       | m          | m              | [26] 20.13                       | i          | c2             |
| 5    | Content-Length  | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6    | Content-Type  | [26] 20.15                       | m          | m              | [26] 20.15                       | i          | c2             |
| 7    | CSeq  | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8    | Date  | [26] 20.17                       | m          | m              | [26] 20.17                       | c1         | c1             |
| 9    | From  | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 10   | MIME-Version  | [26] 20.24                       | m          | m              | [26] 20.24                       | i          | c2             |
| 10A  | P-Access-Network-Info   | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c9         | c9             | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c10        | c10            |
| 10B  | P-Charging-Function-Addresses   | [52] 4.5,<br>[52A] 4             | c7         | c7             | [52] 4.5,<br>[52A] 4             | c8         | c8             |
| 10C  | P-Charging-Vector   | [52] 4.6,<br>[52A] 4             | c5         | n/a            | [52] 4.6,<br>[52A] 4             | c6         | n/a            |
| 10E  | Privacy   | [33] 4.2                         | c3         | c3             | [33] 4.2                         | c4         | c4             |
| 10F  | Recv-Info   | [25] 5.2.3                       | c14        | c14            | [25] 5.2.3                       | c15        | c15            |
| 10G  | Require   | [26] 20.32                       | m          | m              | [26] 20.32                       | c11        | c11            |
| 10H  | Server  | [26] 20.35                       | m          | m              | [26] 20.35                       | i          | i              |
| 10J  | Session-ID  | [162]                            | c16        | c16            | [162]                            | c16        | c16            |
| 11   | Timestamp   | [26] 20.38                       | m          | m              | [26] 20.38                       | i          | i              |
| 12   | To  | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 12A  | User-Agent  | [26] 20.41                       | m          | m              | [26] 20.41                       | i          | i              |
| 13   | Via   | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 14   | Warning   | [26] 20.43                       | m          | m              | [26] 20.43                       | i          | i              |
| c1:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c2:  | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.   |                                  |            |                |                                  |            |                |
| c3:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |                                  |            |                |                                  |            |                |
| c4:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |                                  |            |                |                                  |            |                |
| c5:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |                                  |            |                |                                  |            |                |
| c6:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c7:  | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |                                  |            |                |                                  |            |                |
| c8:  | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |                                  |            |                |                                  |            |                |
| c9:  | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |                                  |            |                |                                  |            |                |
| c10: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |                                  |            |                |                                  |            |                |
| c11: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |                                  |            |                |                                  |            |                |
| c14: | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |                                  |            |                |                                  |            |                |
| c15: | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |                                  |            |                |                                  |            |                |
| c16: | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.251: Supported header fields within the PRACK response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Allow-Events  | [28] 7.2.2 | m          | m              | [28] 7.2.2 | c1         | c1             |
| 0B   | Authentication-Info   | [26] 20.6  | m          | m              | [26] 20.6  | i          | i              |
| 0C   | Accept-Resource-Priority  | [116] 3.2  | c12        | c12            | [116] 3.2  | c12        | c12            |
| 0D   | P-Early-Media   | [109] 8    | o          | c4             | [109] 8    | o          | c5             |
| 1    | Record-Route  | [26] 20.30 | m          | m              | [26] 20.30 | c3         | c3             |
| 2    | Recv-Info   | [25] 5.2.3 | c6         | c6             | [25] 5.2.3 | c7         | c7             |
| 3    | Supported   | [26] 20.37 | m          | m              | [26] 20.37 | i          | i              |
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |            |            |                |            |            |                |
| c3:  | IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routing. |            |            |                |            |            |                |
| c4:  | IF A.162/76 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.                                      |            |            |                |            |            |                |
| c5:  | IF A.162/76 THEN (IF A.3/2 THEN m ELSE i) ELSE n/a - - P-CSCF, using the information in the P-Early-Media header.                                     |            |            |                |            |            |                |
| c6:  | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |            |            |                |            |            |                |
| c7:  | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |            |            |                |            |            |                |
| c12: | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.   |            |            |                |            |            |                |

Prerequisite A.163/3 - - PRACK response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.251A: Supported header fields within the PRACK response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | m          | m              | [26] 20.18 | i          | i              |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.252: Supported header fields within the PRACK response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | c1         | c1             |
| c1:  | IF A.162/19E THEN m ELSE i - - deleting Contact headers. |            |            |                |            |            |                |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.253: Supported header fields within the PRACK response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 8    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.254: Supported header fields within the PRACK response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |

**Table A.255: Void**

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.256: Supported header fields within the PRACK response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 6    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.257: Supported header fields within the PRACK response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1 | m          | m              | [26] 20.1 | i          | i              |
| 2    | Accept-Encoding | [26] 20.2 | m          | m              | [26] 20.2 | i          | i              |
| 3    | Accept-Language | [26] 20.3 | m          | m              | [26] 20.3 | i          | i              |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.257A: Supported header fields within the PRACK response**

| Item | Header field  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority  | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/27 - - Addition for 420 (Bad Extension) response

**Table A.258: Supported header fields within the PRACK response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | c3         | c3             |
| c3:  | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. |            |            |                |            |            |                |

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.258A: Supported header fields within the PRACK response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | c1         | c1             | [48] 2    | n/a        | n/a            |
| c1:  | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

**Table A.259: Void**

Prerequisite A.163/15 - - PRACK response

**Table A.260: Supported message bodies within the PRACK response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

## A.2.2.4.10A PUBLISH method

Prerequisite A.163/15A - - PUBLISH request

Table A.260A: Supported header fields within the PUBLISH request

| Item | Header field                  | Sending                        |            |                | Receiving                      |            |                |
|------|-------------------------------|--------------------------------|------------|----------------|--------------------------------|------------|----------------|
|      |                               | Ref.                           | RFC status | Profile status | Ref.                           | RFC status | Profile status |
| 1    | Accept-Contact                | [56B] 9.2                      | c28        | c28            | [56B] 9.2                      | c28        | c29            |
| 2    | Allow                         | [26] 20.5                      | m          | m              | [26] 20.5                      | i          | i              |
| 3    | Allow-Events                  | [28] 7.2.2                     | m          | m              | [28] 7.2.2                     | c29        | c29            |
| 4    | Authorization                 | [26] 20.7                      | m          | m              | [26] 20.7                      | i          | i              |
| 5    | Call-ID                       | [26] 20.8                      | m          | m              | [26] 20.8                      | m          | m              |
| 6    | Call-Info                     | [26] 24.9                      | m          | m              | [26] 24.9                      | c4         | c4             |
| 6A   | Contact                       | [26] 20.10                     | o          | o              | [26] 20.10                     | o          | o              |
| 7    | Content-Disposition           | [26] 20.11                     | m          | m              | [26] 20.11                     | i          | i              |
| 8    | Content-Encoding              | [26] 20.12                     | m          | m              | [26] 20.12                     | i          | i              |
| 9    | Content-Language              | [26] 20.13                     | m          | m              | [26] 20.13                     | i          | i              |
| 10   | Content-Length                | [26] 20.14                     | m          | m              | [26] 20.14                     | m          | m              |
| 11   | Content-Type                  | [26] 20.15                     | m          | m              | [26] 20.15                     | i          | i              |
| 12   | CSeq                          | [26] 20.16                     | m          | m              | [26] 20.16                     | m          | m              |
| 13   | Date                          | [26] 20.17                     | m          | m              | [26] 20.17                     | c2         | c2             |
| 14   | Event                         | [70] 4, 6                      | m          | m              | [70] 4, 6                      | m          | m              |
| 15   | Expires                       | [26] 20.19,<br>[70] 4, 5,<br>6 | m          | m              | [26] 20.19,<br>[70] 4, 5,<br>6 | i          | i              |
| 15A  | Feature-Caps                  | [190]                          | c70        | c70            | [190]                          | c70        | c70            |
| 16   | From                          | [26] 20.20                     | m          | m              | [26] 20.20                     | m          | m              |
| 16A  | Geolocation                   | [89] 4.1                       | c46        | c46            | [89] 4.1                       | c47        | c47            |
| 16B  | Geolocation-Routing           | [89] 4.1                       | c46        | c46            | [89] 4.1                       | c47        | c47            |
| 16C  | History-Info                  | [66] 4.1                       | c32        | c32            | [66] 4.1                       | c32        | c32            |
| 17   | In-Reply-To                   | [26] 20.21                     | m          | m              | [26] 20.21                     | i          | i              |
| 17A  | Max-Breadth                   | [117] 5.8                      | c44        | c44            | [117] 5.8                      | c45        | c45            |
| 18   | Max-Forwards                  | [26] 20.22                     | m          | m              | [26] 20.22                     | m          | m              |
| 19   | MIME-Version                  | [26] 20.24                     | m          | m              | [26] 20.24                     | i          | i              |
| 20   | Organization                  | [26] 20.25                     | m          | m              | [26] 20.25                     | c3         | c3             |
| 21   | P-Access-Network-Info         | [52] 4.4,<br>[234] 2           | c23        | c23            | [52] 4.4,<br>[234] 2           | c24        | c24            |
| 22   | P-Asserted-Identity           | [34] 9.1                       | c10        | c10            | [34] 9.1                       | c11        | c11            |
| 22A  | P-Asserted-Service            | [121] 4.1                      | c38        | c38            | [121] 4.1                      | c39        | c39            |
| 23   | P-Called-Party-ID             | [52] 4.2                       | c14        | c14            | [52] 4.2                       | c15        | c16            |
| 24   | P-Charging-Function-Addresses | [52] 4.5                       | c21        | c21            | [52] 4.5                       | c22        | c22            |
| 25   | P-Charging-Vector             | [52] 4.6                       | c19        | c19            | [52] 4.6                       | c20        | c20            |
| 26   | P-Preferred-Identity          | [34] 9.2                       | x          | c69            | [34] 9.2                       | c9         | c9             |

|     |                              |                |     |     |                |     |     |
|-----|------------------------------|----------------|-----|-----|----------------|-----|-----|
| 26A | P-Preferred-Service          | [121] 4.2      | x   | x   | [121] 4.2      | c37 | c37 |
| 26B | P-Private-Network-Indication | [134]          | c40 | c40 | [134]          | c40 | c40 |
| 26C | P-Profile-Key                | [97] 5         | c34 | c34 | [97] 5         | c35 | c35 |
| 26D | P-Served-User                | [133] 6        | c41 | c41 | [133] 6        | c41 | c41 |
| 26E | P-User-Database              | [82] 4         | c33 | c33 | [82] 4         | c33 | c33 |
| 27  | P-Visited-Network-ID         | [52] 4.3       | c17 | n/a | [52] 4.3       | c18 | n/a |
| 28  | Priority                     | [26] 20.26     | m   | m   | [26] 20.26     | i   | i   |
| 29  | Privacy                      | [33] 4.2       | c12 | c12 | [33] 4.2       | c13 | c13 |
| 30  | Proxy-Authorization          | [26] 20.28     | m   | m   | [26] 20.28     | c7  | c7  |
| 31  | Proxy-Require                | [26] 20.29     | m   | m   | [26] 20.29     | m   | m   |
| 32  | Reason                       | [34A] 2        | c8  | c8  | [34A] 2        | c1  | c1  |
| 33  | Referred-By                  | [59] 3         | c30 | c30 | [59] 3         | c31 | c31 |
| 34  | Reject-Contact               | [56B] 9.2      | c27 | c27 | [56B] 9.2      | c27 | c28 |
| 34A | Reply-To                     | [26] 20.31     | m   | m   | [26] 20.31     | i   | i   |
| 35  | Request-Disposition          | [56B] 9.1      | c27 | c27 | [56B] 9.1      | c27 | c27 |
| 36  | Require                      | [26] 20.32     | m   | m   | [26] 20.32     | c5  | c5  |
| 36A | Resource-Priority            | [116] 3.1      | c36 | c36 | [116] 3.1      | c36 | c36 |
| 37  | Route                        | [26] 20.34     | m   | m   | [26] 20.34     | m   | m   |
| 38  | Security-Client              | [48] 2.3.1     | x   | x   | [48] 2.3.1     | c25 | c25 |
| 39  | Security-Verify              | [48] 2.3.1     | x   | x   | [48] 2.3.1     | c25 | c25 |
| 39A | Session-ID                   | [162]          | c48 | c48 | [162]          | c48 | c48 |
| 40  | SIP-If-Match                 | [70]<br>11.3.2 | m   | m   | [70]<br>11.3.2 | i   | i   |
| 41  | Subject                      | [26] 20.36     | m   | m   | [26] 20.36     | i   | i   |
| 42  | Supported                    | [26] 20.37     | m   | m   | [26] 20.37     | c6  | c6  |
| 43  | Timestamp                    | [26] 20.38     | m   | m   | [26] 20.38     | i   | i   |
| 44  | To                           | [26] 20.39     | m   | m   | [26] 20.39     | m   | m   |
| 45  | User-Agent                   | [26] 20.41     | m   | m   | [26] 20.41     | i   | i   |
| 46  | Via                          | [26] 20.42     | m   | m   | [26] 20.42     | m   | m   |



|      |   |
|------|---|
| c1:  | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c2:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c3:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |
| c4:  | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |
| c5:  | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6:  | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.  |
| c7:  | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.  |
| c8:  | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c9:  | IF A.162/30A OR A.162/30C THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity, act as entity passing on identity transparently independent of trust domain.   |
| c10: | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c11: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |
| c12: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c13: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c14: | IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension.   |
| c15: | IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension.   |
| c16: | IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND (A.3/3 OR A.3/9A) THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or (I-CSCF or IBCF (THIG)).   |
| c17: | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension.  |
| c18: | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response.   |
| c19: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c20: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c21: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c22: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c23: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c24: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c25: | IF A.162/47 OR A.162/47A THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media (note 1).   |
| c27: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c28: | IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CSCF.   |
| c29: | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension (note 2).   |
| c30: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.  |
| c31: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c32: | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c33: | IF A.162/60 THEN m ELSE n/a - - the P-User-Database private header extension.   |
| c34: | IF A.162/66A THEN m ELSE n/a - - making the first query to the database in order to populate the P-Profile-Key header.  |
| c35: | IF A.162/66B THEN m ELSE n/a - - using the information in the P-Profile-Key header.   |
| c36: | IF A.162/80B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.  |
| c37: | IF A.162/84A THEN m ELSE n/a - - act as authentication entity within the trust domain for asserted service.   |
| c38: | IF A.162/84 THEN m ELSE n/a - - SIP extension for the identification of services.   |
| c39: | IF A.162/84 OR A.162/30B THEN m ELSE i - - SIP extension for the identification of services or subsequent entity within trust network that can route outside the trust network.   |
| c40: | IF A.162/87 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).   |
| c41: | IF A.162/88 THEN m ELSE n/a - - the SIP P-Served-User private header.   |

|         |  |
|---------|--|
| c44:    | IF A.162/81 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.  |
| c45:    | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, forking of initial requests. |
| c46:    | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.   |
| c47:    | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.                                    |
| c48:    | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.  |
| c69:    | IF A.162/30C THEN m ELSE x - - act as entity passing on identity transparently independent of trust domain.  |
| c70:    | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.  |
| NOTE 1: | Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented.   |
| NOTE 2: | c29 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.  |

Prerequisite A.163/15A - - PUBLISH request

**Table A.260B: Supported message bodies within the PUBLISH request**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/1 - - Additional for 100 (Trying) response

**Table A.260BA: Supported header fields within the PUBLISH response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID   | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length  | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq  | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date  | [26] 20.17 | c1         | c1             | [26] 20.17 | c2         | c2             |
| 5    | From  | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To  | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies. |            |            |                |            |            |                |
| c2:  | IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.   |            |            |                |            |            |                |

Prerequisite A.163/15B - - PUBLISH response for all remaining status-codes

**Table A.260C: Supported header fields within the PUBLISH response**

| Item | Header field                  | Sending                          |            |                | Receiving                        |            |                |
|------|-------------------------------|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |                               | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow                         | [26] 20.5                        | m          | m              | [26] 20.5                        | i          | i              |
| 1    | Call-ID                       | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 2    | Call-Info                     | [26] 24.9                        | m          | m              | [26] 24.9                        | c3         | c3             |
| 3    | Content-Disposition           | [26] 20.11                       | m          | m              | [26] 20.11                       | i          | i              |
| 4    | Content-Encoding              | [26] 20.12                       | m          | m              | [26] 20.12                       | i          | i              |
| 5    | Content-Language              | [26] 20.13                       | m          | m              | [26] 20.13                       | i          | i              |
| 6    | Content-Length                | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 7    | Content-Type                  | [26] 20.15                       | m          | m              | [26] 20.15                       | i          | i              |
| 8    | CSeq                          | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 9    | Date                          | [26] 20.17                       | m          | m              | [26] 20.17                       | c1         | c1             |
| 10   | From                          | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 10A  | Geolocation-Error             | [89] 4.3                         | c19        | c19            | [89] 4.3                         | c20        | c20            |
| 10B  | History-Info                  | [66] 4.1                         | c16        | c16            | [66] 4.1                         | c16        | c16            |
| 11   | MIME-Version                  | [26] 20.24                       | m          | m              | [26] 20.24                       | i          | i              |
| 12   | Organization                  | [26] 20.25                       | m          | m              | [26] 20.25                       | c2         | c2             |
| 13   | P-Access-Network-Info         | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c13        | c13            | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c14        | c14            |
| 14   | P-Asserted-Identity           | [34] 9.1                         | c5         | c5             | [34] 9.1                         | c6         | c6             |
| 15   | P-Charging-Function-Addresses | [52] 4.5,<br>[52A] 4             | c11        | c11            | [52] 4.5,<br>[52A] 4             | c12        | c12            |
| 16   | P-Charging-Vector             | [52] 4.6,<br>[52A] 4             | c9         | n/a            | [52] 4.6,<br>[52A] 4             | c10        | n/a            |
| 17   | P-Preferred-Identity          | [34] 9.2                         | x          | x              | [34] 9.2                         | c4         | n/a            |
| 18   | Privacy                       | [33] 4.2                         | c7         | c7             | [33] 4.2                         | c8         | c8             |
| 19   | Require                       | [26] 20.32                       | m          | m              | [26] 20.32                       | c15        | c15            |
| 20   | Server                        | [26] 20.35                       | m          | m              | [26] 20.35                       | i          | i              |
| 20A  | Session-ID                    | [162]                            | c21        | c21            | [162]                            | c21        | c21            |
| 21   | Timestamp                     | [26] 20.38                       | m          | m              | [26] 20.38                       | i          | i              |
| 22   | To                            | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 23   | User-Agent                    | [26] 20.41                       | m          | m              | [26] 20.41                       | i          | i              |
| 24   | Via                           | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 25   | Warning                       | [26] 20.43                       | m          | m              | [26] 20.43                       | i          | i              |

|      |   |
|------|---|
| c1:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c2:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |
| c3:  | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |
| c4:  | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.   |
| c5:  | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c6:  | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |
| c7:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c8:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c9:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c10: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c11: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c12: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c13: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c14: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c15: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c16: | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c19: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c20: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c21: | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/7 - - Additional for 200 (OK) response

**Table A.260D: Supported header fields within the PUBLISH response**

| Item | Header field   | Sending                           |            |                | Receiving                         |            |                |
|------|--|-----------------------------------|------------|----------------|-----------------------------------|------------|----------------|
|      |  | Ref.                              | RFC status | Profile status | Ref.                              | RFC status | Profile status |
| 1    | Accept-Resource-Priority   | [116] 3.2                         | c4         | c4             | [116] 3.2                         | c4         | c4             |
| 1A   | Allow-Events   | [28] 7.2.2                        | m          | m              | [28] 7.2.2                        | c1         | c1             |
| 2    | Authentication-Info  | [26] 20.6                         | m          | m              | [26] 20.6                         | i          | i              |
| 3    | Expires  | [26]<br>20.19,<br>[70] 4, 5,<br>6 | m          | m              | [26]<br>20.19,<br>[70] 4, 5,<br>6 | i          | i              |
| 3A   | Feature-Caps   | [190]                             | c6         | c6             | [190]                             | c6         | c6             |
| 4    | SIP-Etag   | [70]<br>11.3.1                    | m          | m              | [70]<br>11.3.1                    | i          | i              |
| 5    | Supported  | [26] 20.37                        | m          | m              | [26] 20.37                        | i          | i              |
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.   |                                   |            |                |                                   |            |                |
| c4:  | IF A.162/80B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol. |                                   |            |                |                                   |            |                |
| c6:  | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.  |                                   |            |                |                                   |            |                |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.260DA: Supported header fields within the PUBLISH response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | m          | m              | [26] 20.18 | i          | i              |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.260E: Supported header fields within the PUBLISH response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | c1         | c1             |
| c1:  | IF A.162/19E THEN m ELSE i - - deleting Contact headers. |            |            |                |            |            |                |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 - - Additional for 401 (Unauthorized) response

**Table A.260F: Supported header fields within the PUBLISH response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 5    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.260G: Supported header fields within the PUBLISH response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |

**Table A.260H: Void**

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.260I: Supported header fields within the PUBLISH response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 5    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.260J: Supported header fields within the PUBLISH response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1 | m          | m              | [26] 20.1 | i          | i              |
| 2    | Accept-Encoding | [26] 20.2 | m          | m              | [26] 20.2 | i          | i              |
| 3    | Accept-Language | [26] 20.3 | m          | m              | [26] 20.3 | i          | i              |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.260JA: Supported header fields within the PUBLISH response**

| Item | Header field   | Sending   |            |                | Receiving |            |                |
|------|--|-----------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority   | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.162/80B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.260K: Supported header fields within the PUBLISH response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | c3         | c3             |
| c3:  | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. |            |            |                |            |            |                |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.260L: Supported header fields within the PUBLISH response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | c1         | c1             | [48] 2    | n/a        | n/a            |
| c1:  | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/29 - - Additional for 423 (Interval Too Brief) response

**Table A.260M: Supported header fields within the PUBLISH response**

| Item | Header field | Sending                     |            |                | Receiving                   |            |                |
|------|--------------|-----------------------------|------------|----------------|-----------------------------|------------|----------------|
|      |              | Ref.                        | RFC status | Profile status | Ref.                        | RFC status | Profile status |
| 3    | Min-Expires  | [26]<br>20.23,<br>[70] 5, 6 | m          | m              | [26]<br>20.23,<br>[70] 5, 6 | i          | i              |

**Table A.260N: Void**

Prerequisite A.163/15B - - PUBLISH response

Prerequisite: A.164/39 - - Additional for 489 (Bad Event) response

**Table A.260O: Supported header fields within the PUBLISH response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Allow-Events | [28] 8.2.2 | m          | m              | [28] 8.2.2 | i          | i              |

Prerequisite A.163/17 - - PUBLISH response

**Table A.260P: Supported message bodies within the PUBLISH response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |



#### A.2.2.4.11 REFER method

Prerequisite A.163/16 - - REFER request

**Table A.261: Supported header fields within the REFER request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 0A   | Accept                        | [26] 20.1            | m          | m              | [26] 20.1            | i          | i              |
| 0B   | Accept-Contact                | [56B] 9.2            | c27        | c27            | [56B] 9.2            | c27        | c28            |
| 0C   | Accept-Encoding               | [26] 20.2            | m          | m              | [26] 20.2            | i          | i              |
| 1    | Accept-Language               | [26] 20.3            | m          | m              | [26] 20.3            | i          | i              |
| 1A   | Allow                         | [26] 20.5            | m          | m              | [26] 20.5            | i          | i              |
| 2    | Allow-Events                  | [28] 7.2.2           | m          | m              | [28] 7.2.2           | c1         | c1             |
| 3    | Authorization                 | [26] 20.7            | m          | m              | [26] 20.7            | i          | i              |
| 4    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 5    | Contact                       | [26] 20.10           | m          | m              | [26] 20.10           | i          | i              |
| 5A   | Content-Disposition           | [26] 20.11           | m          | m              | [26] 20.11           | i          | i              |
| 5B   | Content-Encoding              | [26] 20.12           | m          | m              | [26] 20.12           | i          | i              |
| 5C   | Content-Language              | [26] 20.13           | m          | m              | [26] 20.13           | i          | i              |
| 6    | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 7    | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | i          | i              |
| 8    | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 9    | Date                          | [26] 20.17           | m          | m              | [26] 20.17           | c2         | c2             |
| 10   | Expires                       | [26] 20.19           | m          | m              | [26] 20.19           | i          | i              |
| 10A  | Feature-Caps                  | [190]                | cj         | cj             | [190]                | cj         | cj             |
| 11   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 11A  | Geolocation                   | [89] 4.1             | c35        | c35            | [89] 4.1             | c36        | c36            |
| 11B  | Geolocation-Routing           | [89] 4.1             | c35        | c35            | [89] 4.1             | c36        | c36            |
| 11C  | History-Info                  | [66] 4.1             | c31        | c31            | [66] 4.1             | c31        | c31            |
| 11D  | Max-Breadth                   | [117] 5.8            | c40        | c40            | [117] 5.8            | c41        | c41            |
| 12   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | m          | m              |
| 13   | MIME-Version                  | [26] 20.24           | m          | m              | [26] 20.24           | i          | i              |
| 14   | Organization                  | [26] 20.25           | m          | m              | [26] 20.25           | c3         | c3             |
| 14A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c22        | c22            | [52] 4.4,<br>[234] 2 | c23        | c23            |
| 14B  | P-Asserted-Identity           | [34] 9.1             | c9         | c9             | [34] 9.1             | c10        | c10            |
| 14C  | P-Asserted-Service            | [121] 4.1            | c38        | c38            | [121] 4.1            | c39        | c39            |
| 14D  | P-Called-Party-ID             | [52] 4.2,<br>[52A] 4 | c13        | c13            | [52] 4.2,<br>[52A] 4 | c14        | c15            |
| 14E  | P-Charging-Function-Addresses | [52] 4.5             | c20        | c20            | [52] 4.5             | c21        | c21            |
| 14F  | P-Charging-Vector             | [52] 4.6             | c18        | c18            | [52] 4.6             | c19        | c19            |
| 14H  | P-Preferred-Identity          | [34] 9.2             | x          | c69            | [34] 9.2             | c8         | c8             |
| 14I  | P-Preferred-Service           | [121] 4.2            | x          | x              | [121] 4.2            | c37        | c37            |
| 14J  | P-Private-Network-Indication  | [134]                | c50        | c50            | [134]                | c50        | c50            |
| 14K  | P-Profile-Key                 | [97] 5               | c33        | c33            | [97] 5               | c34        | c34            |
| 14L  | P-Served-User                 | [133] 6              | c53        | c53            | [133] 6              | c53        | c53            |
| 14M  | P-User-Database               | [82] 4               | c32        | c32            | [82] 4               | c32        | c32            |
| 14N  | P-Visited-Network-ID          | [52] 4.3             | c16        | n/a            | [52] 4.3             | c17        | n/a            |
| 14O  | Privacy                       | [33] 4.2             | c11        | c11            | [33] 4.2             | c12        | c12            |
| 15   | Proxy-Authorization           | [26] 20.28           | m          | m              | [26] 20.28           | c4         | c4             |
| 16   | Proxy-Require                 | [26] 20.29           | m          | m              | [26] 20.29           | m          | m              |
| 16A  | Reason                        | [34A] 2              | c25        | c25            | [34A] 2              | c26        | c26            |
| 17   | Record-Route                  | [26] 20.30           | m          | m              | [26] 20.30           | c7         | c7             |
| 17A  | Refer-Sub                     | [173] 4              | c54        | c54            | [173] 4              | c55        | c55            |
| 18   | Refer-To                      | [36] 3               | c3         | c3             | [36] 3               | c4         | c4             |
| 18A  | Referred-By                   | [59] 3               | c29        | c29            | [59] 3               | c30        | c30            |
| 18B  | Reject-Contact                | [56B] 9.2            | c27        | c27            | [56B] 9.2            | c27        | c28            |
| 18C  | Request-Disposition           | [56B] 9.1            | c27        | c27            | [56B] 9.1            | c27        | c27            |
| 19   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | c5         | c5             |
| 19A  | Resource-Priority             | [116] 3.1            | c47        | c47            | [116] 3.1            | c47        | c47            |
| 20   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | m          | m              |
| 20A  | Security-Client               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c24        | c24            |
| 20B  | Security-Verify               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c24        | c24            |
| 20C  | Session-ID                    | [162]                | c70        | c70            | [162]                | c70        | c70            |
| 21   | Supported                     | [26] 20.37           | m          | m              | [26] 20.37           | c6         | c6             |
| 21A  | Target-Dialog                 | [184] 7              | c71        | c71            | [184] 7              | c72        | c72            |
| 22   | Timestamp                     | [26] 20.38           | m          | m              | [26] 20.38           | i          | i              |
| 23   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |

|      |   |                 |     |     |                 |     |     |
|------|---|-----------------|-----|-----|-----------------|-----|-----|
| 23A  | Trigger-Consent   | [125]<br>5.11.2 | c48 | c48 | [125]<br>5.11.2 | c49 | c49 |
| 24   | User-Agent  | [26] 20.41      | m   | m   | [26] 20.41      | i   | i   |
| 25   | Via   | [26] 20.42      | m   | m   | [26] 20.42      | m   | m   |
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |                 |     |     |                 |     |     |
| c2:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |                 |     |     |                 |     |     |
| c3:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |                 |     |     |                 |     |     |
| c4:  | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.  |                 |     |     |                 |     |     |
| c5:  | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |                 |     |     |                 |     |     |
| c6:  | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.  |                 |     |     |                 |     |     |
| c7:  | IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.   |                 |     |     |                 |     |     |
| c8:  | IF A.162/30A OR A.162/30C THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity, act as entity passing on identity transparently independent of trust domain.   |                 |     |     |                 |     |     |
| c9:  | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |                 |     |     |                 |     |     |
| c10: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |                 |     |     |                 |     |     |
| c11: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |                 |     |     |                 |     |     |
| c12: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |                 |     |     |                 |     |     |
| c13: | IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension.   |                 |     |     |                 |     |     |
| c14: | IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension.   |                 |     |     |                 |     |     |
| c15: | IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND (A.3/3 OR A.3/9A) THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or (I-CSCF or IBCF (THIG)).   |                 |     |     |                 |     |     |
| c16: | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension.  |                 |     |     |                 |     |     |
| c17: | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response.   |                 |     |     |                 |     |     |
| c18: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |                 |     |     |                 |     |     |
| c19: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |                 |     |     |                 |     |     |
| c20: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |                 |     |     |                 |     |     |
| c21: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |                 |     |     |                 |     |     |
| c22: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |                 |     |     |                 |     |     |
| c23: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |                 |     |     |                 |     |     |
| c24: | IF A.162/47 OR A.162/47A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |                 |     |     |                 |     |     |
| c25: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |                 |     |     |                 |     |     |
| c26: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.  |                 |     |     |                 |     |     |
| c27: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |                 |     |     |                 |     |     |
| c28: | IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CSCF.   |                 |     |     |                 |     |     |
| c29: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.  |                 |     |     |                 |     |     |
| c30: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |                 |     |     |                 |     |     |
| c31: | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |                 |     |     |                 |     |     |
| c32: | IF A.162/60 THEN m ELSE n/a - - the P-User-Database private header extension.   |                 |     |     |                 |     |     |
| c33: | IF A.162/66A THEN m ELSE n/a - - making the first query to the database in order to populate the P-Profile-Key header.  |                 |     |     |                 |     |     |
| c34: | IF A.162/66B THEN m ELSE n/a - - using the information in the P-Profile-Key header.   |                 |     |     |                 |     |     |
| c35: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |                 |     |     |                 |     |     |
| c36: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |                 |     |     |                 |     |     |
| c37: | IF A.162/84A THEN m ELSE n/a - - act as authentication entity within the trust domain for asserted service.   |                 |     |     |                 |     |     |
| c38: | IF A.162/84 THEN m ELSE n/a - - SIP extension for the identification of services.   |                 |     |     |                 |     |     |
| c39: | IF A.162/84 OR A.162/30B THEN m ELSE i - - SIP extension for the identification of services or subsequent entity within trust network that can route outside the trust network.   |                 |     |     |                 |     |     |

|       |  |
|-------|--|
| c40:  | IF A.162/81 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.  |
| c41:  | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, forking of initial requests. |
| c47:  | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.  |
| c48:  | IF A.162/85 THEN m ELSE n/a - - a framework for consent-based communications in SIP.   |
| c49:  | IF A.162/85 THEN i ELSE n/a - - a framework for consent-based communications in SIP.   |
| c50:  | IF A.162/87 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).  |
| c53:  | IF A.162/88 THEN m ELSE n/a - - the SIP P-Served-User private header.  |
| c54:  | IF A.162/105 THEN m ELSE n/a - - suppression of session initiation protocol REFER method implicit subscription.  |
| c55:  | IF A.162/105 THEN i ELSE n/a - - suppression of session initiation protocol REFER method implicit subscription.  |
| c69:  | IF A.162/30C THEN m ELSE x - - act as entity passing on identity transparently independent of trust domain.  |
| c70:  | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.  |
| c71:  | IF A.162/109 THEN m ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.   |
| c72:  | IF A.162/109 THEN i ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.   |
| c73:  | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.  |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.   |

Prerequisite A.163/16 - - REFER request

**Table A.262: Supported message bodies within the REFER request**

| Item | Header                            | Sending |            |                | Receiving |            |                |
|------|-----------------------------------|---------|------------|----------------|-----------|------------|----------------|
|      |                                   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | application/vnd.3gpp.mid-call+xml | [8M] D  | n/a        | i              | [8M] D    | n/a        | i              |

**Table A.263: Void**

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/1 - - Additional for 100 (Trying) response

**Table A.263A: Supported header fields within the REFER response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID   | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length  | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq  | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date  | [26] 20.17 | c1         | c1             | [26] 20.17 | c2         | c2             |
| 5    | From  | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To  | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies. |            |            |                |            |            |                |
| c2:  | IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.   |            |            |                |            |            |                |

Prerequisite A.163/17 - - REFER response for all remaining status-codes

**Table A.264: Supported header fields within the REFER response**

| Item | Header field                  | Sending                          |            |                | Receiving                        |            |                |
|------|-------------------------------|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |                               | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow                         | [26] 20.5                        | m          | m              | [26] 20.5                        | i          | i              |
| 1    | Call-ID                       | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 1A   | Contact                       | [26] 20.10                       | m          | m              | [26] 20.10                       | i          | i              |
| 1B   | Content-Disposition           | [26] 20.11                       | m          | m              | [26] 20.11                       | i          | i              |
| 2    | Content-Encoding              | [26] 20.12                       | m          | m              | [26] 20.12                       | i          | i              |
| 3    | Content-Language              | [26] 20.13                       | m          | m              | [26] 20.13                       | i          | i              |
| 4    | Content-Length                | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 5    | Content-Type                  | [26] 20.15                       | m          | m              | [26] 20.15                       | i          | i              |
| 6    | CSeq                          | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 7    | Date                          | [26] 20.17                       | m          | m              | [26] 20.17                       | c1         | c1             |
| 8    | From                          | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 8A   | Geolocation-Error             | [89] 4.3                         | c16        | c16            | [89] 4.3                         | c17        | c17            |
| 8B   | History-Info                  | [66] 4.1                         | c15        | c15            | [66] 4.1                         | c15        | c15            |
| 9    | MIME-Version                  | [26] 20.24                       | m          | m              | [26] 20.24                       | i          | i              |
| 10   | Organization                  | [26] 20.25                       | m          | m              | [26] 20.25                       | c2         | c2             |
| 10A  | P-Access-Network-Info         | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c12        | c12            | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c13        | c13            |
| 10B  | P-Asserted-Identity           | [34] 9.1                         | c4         | c4             | [34] 9.1                         | c5         | c5             |
| 10C  | P-Charging-Function-Addresses | [52] 4.5,<br>[52A] 4             | c10        | c10            | [52] 4.5,<br>[52A] 4             | c11        | c11            |
| 10D  | P-Charging-Vector             | [52] 4.6,<br>[52A] 4             | c8         | c8             | [52] 4.6,<br>[52A] 4             | c9         | c9             |
| 10F  | P-Preferred-Identity          | [34] 9.2                         | x          | x              | [34] 9.2                         | c3         | n/a            |
| 10G  | Privacy                       | [33] 4.2                         | c6         | c6             | [33] 4.2                         | c7         | c7             |
| 10H  | Require                       | [26] 20.32                       | m          | m              | [26] 20.32                       | c14        | c14            |
| 10I  | Server                        | [26] 20.35                       | m          | m              | [26] 20.35                       | i          | i              |
| 10J  | Session-ID                    | [162]                            | c20        | c20            | [162]                            | c20        | c20            |
| 11   | Timestamp                     | [26] 20.38                       | m          | m              | [26] 20.38                       | i          | i              |
| 12   | To                            | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 12A  | User-Agent                    | [26] 20.41                       | m          | m              | [26] 20.41                       | i          | i              |
| 13   | Via                           | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 14   | Warning                       | [26] 20.43                       | m          | m              | [26] 20.43                       | i          | i              |

|      |   |
|------|---|
| c1:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c2:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |
| c3:  | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.   |
| c4:  | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c5:  | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |
| c6:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c7:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c8:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c9:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c10: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c11: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c12: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c13: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c14: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c15: | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c16: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c17: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c20: | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.265: Supported header fields within the REFER response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Accept-Resource-Priority  | [116] 3.2  | c12        | c12            | [116] 3.2  | c12        | c12            |
| 1    | Allow-Events  | [28] 7.2.2 | m          | m              | [28] 7.2.2 | c1         | c1             |
| 2    | Authentication-Info   | [26] 20.6  | m          | m              | [26] 20.6  | i          | i              |
| 3    | Feature-Caps  | [190]      | c14        | c14            | [190]      | c14        | c14            |
| 5    | Record-Route  | [26] 20.30 | m          | m              | [26] 20.30 | c3         | c3             |
| 6    | Refer-Sub   | [173] 4    | c4         | c4             | [173] 4    | c5         | c5             |
| 8    | Supported   | [26] 20.37 | m          | m              | [26] 20.37 | i          | i              |
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |            |            |                |            |            |                |
| c3:  | IF A.162/15 THEN m ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routing. |            |            |                |            |            |                |
| c4:  | IF A.162/105 THEN m ELSE n/a - - suppression of session initiation protocol REFER method implicit subscription.                                       |            |            |                |            |            |                |
| c5:  | IF A.162/105 THEN I ELSE n/a - - suppression of session initiation protocol REFER method implicit subscription.                                       |            |            |                |            |            |                |
| c12: | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.   |            |            |                |            |            |                |
| c14: | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.   |            |            |                |            |            |                |

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.265A: Supported header fields within the REFER response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | m          | m              | [26] 20.18 | i          | i              |

**Table A.266: Void**

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 - - Additional for 401 (Unauthorized) response

**Table A.267: Supported header fields within the REFER response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 10   | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.268: Supported header fields within the REFER response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 6    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |

**Table A.269: Void**

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.270: Supported header fields within the REFER response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Proxy-Authenticate | [26] 20.27 | o          |                | [26] 20.27 | o          |                |
| 8    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |



Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.271: Supported header fields within the REFER response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1 | m          | m              | [26] 20.1 | i          | i              |
| 2    | Accept-Encoding | [26] 20.2 | m          | m              | [26] 20.2 | i          | i              |
| 3    | Accept-Language | [26] 20.3 | m          | m              | [26] 20.3 | i          | i              |

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.271A: Supported header fields within the REFER response**

| Item | Header field  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority  | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.272: Supported header fields within the REFER response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 8    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | c3         | c3             |
| c3:  | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. |            |            |                |            |            |                |

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.272A: Supported header fields within the REFER response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | c1         | c1             | [48] 2    | n/a        | n/a            |
| c1:  | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

**Table A.273: Void**

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/29H - - Additional for 470 (Consent Needed) response

**Table A.273A: Supported header fields within the REFER response**

| Item | Header field       | Sending        |            |                | Receiving      |            |                |
|------|--------------------|----------------|------------|----------------|----------------|------------|----------------|
|      |                    | Ref.           | RFC status | Profile status | Ref.           | RFC status | Profile status |
| 1    | Permission-Missing | [125]<br>5.9.3 | m          | m              | [125]<br>5.9.3 | m          | m              |

Prerequisite A.163/17 - - REFER response

**Table A.274: Supported message bodies within the REFER response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

#### A.2.2.4.12 REGISTER method

Prerequisite A.163/18 - - REGISTER request

**Table A.275: Supported header fields within the REGISTER request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | m          | m              | [26] 20.1            | i          | i              |
| 2    | Accept-Encoding               | [26] 20.2            | m          | m              | [26] 20.2            | i          | i              |
| 3    | Accept-Language               | [26] 20.3            | m          | m              | [26] 20.3            | i          | i              |
| 3A   | Allow                         | [26] 20.5            | m          | m              | [26] 20.5            | i          | i              |
| 4    | Allow-Events                  | [28] 7.2.2           | m          | m              | [28] 7.2.2           | c1         | c1             |
| 5    | Authorization                 | [26] 20.7,<br>[49]   | m          | m              | [26] 20.7,<br>[49]   | i          | i              |
| 6    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 7    | Call-Info                     | [26] 20.9            | m          | m              | [26] 20.9            | c2         | c2             |
| 8    | Contact                       | [26] 20.10           | m          | m              | [26] 20.10           | i          | i              |
| 9    | Content-Disposition           | [26] 20.11           | m          | m              | [26] 20.11           | i          | i              |
| 10   | Content-Encoding              | [26] 20.12           | m          | m              | [26] 20.12           | i          | i              |
| 11   | Content-Language              | [26] 20.13           | m          | m              | [26] 20.13           | i          | i              |
| 12   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 13   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | i          | i              |
| 14   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 15   | Date                          | [26] 20.17           | m          | m              | [26] 20.17           | m          | m              |
| 16   | Expires                       | [26] 20.19           | m          | m              | [26] 20.19           | i          | i              |
| 16A  | Feature-Caps                  | [190]                | c36        | c36            | [190]                | c36        | c36            |
| 17   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 17A  | Geolocation                   | [89] 4.1             | c26        | c26            | [89] 4.1             | c27        | c27            |
| 17B  | Geolocation-Routing           | [89] 4.1             | c26        | c26            | [89] 4.1             | c27        | c27            |
| 17C  | History-Info                  | [66] 4.1             | c24        | c24            | [66] 4.1             | c24        | c24            |
| 17D  | Max-Breadth                   | [117] 5.8            | c31        | c31            | [117] 5.8            | c32        | c32            |
| 18   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | m          | m              |
| 19   | MIME-Version                  | [26] 20.24           | m          | m              | [26] 20.24           | i          | i              |
| 20   | Organization                  | [26] 20.25           | m          | m              | [26] 20.25           | c3         | c3             |
| 20A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c16        | c16            | [52] 4.4,<br>[234] 2 | c17        | c17            |
| 20B  | P-Charging-Function-Addresses | [52] 4.5             | c14        | c14            | [52] 4.5             | c15        | c15            |
| 20C  | P-Charging-Vector             | [52] 4.6             | c12        | c12            | [52] 4.6             | c13        | c13            |
| 20E  | P-User-Database               | [82] 4               | c25        | c25            | [82] 4               | n/a        | n/a            |
| 20F  | P-Visited-Network-ID          | [52] 4.3             | c10        | c10            | [52] 4.3             | c11        | c11            |
| 20G  | Path                          | [35] 4.2             | c6         | c6             | [35] 4.2             | c6         | c6             |
| 20H  | Privacy                       | [33] 4.2             | c8         | c8             | [33] 4.2             | c9         | c9             |
| 21   | Proxy-Authorization           | [26] 20.28           | m          | m              | [26] 20.28           | c7         | c7             |
| 22   | Proxy-Require                 | [26] 20.29           | m          | m              | [26] 20.29           | m          | m              |
| 22A  | Reason                        | [34A] 2              | c19        | c19            | [34A] 2              | c20        | c20            |
| 22B  | Recv-Info                     | [25] 5.2.3           | c33        | c33            | [25] 5.2.3           | c34        | c34            |
| 22C  | Referred-By                   | [59] 3               | c22        | c22            | [59] 3               | c23        | c23            |
| 22D  | Request-Disposition           | [56B] 9.1            | c21        | c21            | [56B] 9.1            | c21        | c21            |
| 23   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | c4         | c4             |
| 23A  | Resource-Priority             | [116] 3.1            | c28        | c28            | [116] 3.1            | c28        | c28            |
| 24   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | m          | m              |
| 24A  | Security-Client               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c18        | c18            |
| 24B  | Security-Verify               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c18        | c18            |
| 24C  | Session-ID                    | [162]                | c35        | c35            | [162]                | c35        | c35            |
| 25   | Supported                     | [26] 20.37           | m          | m              | [26] 20.37           | c5         | c5             |
| 26   | Timestamp                     | [26] 20.38           | m          | m              | [26] 20.38           | i          | i              |
| 27   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 28   | User-Agent                    | [26] 20.41           | m          | m              | [26] 20.41           | i          | i              |
| 29   | Via                           | [26] 20.42           | m          | m              | [26] 20.42           | m          | m              |

|       |   |
|-------|---|
| c1:   | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |
| c2:   | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |
| c3:   | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |
| c4:   | IF A.162/11 OR A.162/12 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c5:   | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.  |
| c6:   | IF A.162/29 THEN m ELSE n/a - - PATH header support.  |
| c7:   | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.  |
| c8:   | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c9:   | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c10:  | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension.  |
| c11:  | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response.   |
| c12:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c13:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c14:  | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c15:  | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c16:  | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c17:  | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c18:  | IF A.162/47 OR 162/47A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |
| c19:  | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c20:  | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c21:  | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c22:  | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.  |
| c23:  | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c24:  | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c25:  | IF A.162/60 THEN m ELSE n/a - - the P-User-Database private header extension.   |
| c26:  | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c27:  | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c28:  | IF A.162/80B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.  |
| c31:  | IF A.162/81 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |
| c32:  | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, forking of initial requests.  |
| c33:  | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |
| c34:  | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |
| c35:  | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |
| c36:  | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.   |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.  |

Prerequisite A.163/18 - - REGISTER request

**Table A.276: Supported message bodies within the REGISTER request**

| Item | Header                        | Sending       |            |                | Receiving     |            |                |
|------|-------------------------------|---------------|------------|----------------|---------------|------------|----------------|
|      |                               | Ref.          | RFC status | Profile status | Ref.          | RFC status | Profile status |
| 1    | 3GPP IM CN subsystem XML body | subclause 7.6 | n/a        | m              | subclause 7.6 | n/a        | i              |

**Table A.277: Void**

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/1 - - Additional for 100 (Trying) response

**Table A.277A: Supported header fields within the REGISTER response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID   | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length  | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq  | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date  | [26] 20.17 | c1         | c1             | [26] 20.17 | c2         | c2             |
| 5    | From  | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To  | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies. |            |            |                |            |            |                |
| c2:  | IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.   |            |            |                |            |            |                |

Prerequisite A.163/19 - - REGISTER response for all remaining status-codes

**Table A.278: Supported header fields within the REGISTER response**

| Item | Header field  | Sending                          |            |                | Receiving                        |            |                |
|------|---|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |   | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow   | [26] 20.5                        | m          | m              | [26] 20.5                        | i          | i              |
| 1    | Call-ID   | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 1A   | Call-Info   | [26] 20.9                        | m          | m              | [26] 20.9                        | c2         | c2             |
| 2    | Content-Disposition   | [26] 20.11                       | m          | m              | [26] 20.11                       | i          | i              |
| 3    | Content-Encoding  | [26] 20.12                       | m          | m              | [26] 20.12                       | i          | i              |
| 4    | Content-Language  | [26] 20.13                       | m          | m              | [26] 20.13                       | i          | i              |
| 5    | Content-Length  | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6    | Content-Type  | [26] 20.15                       | m          | m              | [26] 20.15                       | i          | i              |
| 7    | CSeq  | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8    | Date  | [26] 20.17                       | m          | m              | [26] 20.17                       | m          | m              |
| 9    | From  | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A   | Geolocation-Error   | [89] 4.3                         | c13        | c13            | [89] 4.3                         | c14        | c14            |
| 9B   | History-Info  | [66] 4.1                         | c12        | c12            | [66] 4.1                         | c12        | c12            |
| 10   | MIME-Version  | [26] 20.24                       | m          | m              | [26] 20.24                       | i          | i              |
| 11   | Organization  | [26] 20.25                       | m          | m              | [26] 20.25                       | c1         | c1             |
| 11A  | P-Access-Network-Info   | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c9         | c9             | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c10        | c10            |
| 11B  | P-Charging-Function-Addresses   | [52] 4.5,<br>[52A] 4             | c7         | c7             | [52] 4.5,<br>[52A] 4             | c8         | c8             |
| 11C  | P-Charging-Vector   | [52] 4.6,<br>[52A] 4             | c5         | c5             | [52] 4.6,<br>[52A] 4             | c6         | c6             |
| 11E  | Privacy   | [33] 4.2                         | c3         | c3             | [33] 4.2                         | c4         | c4             |
| 11F  | Require   | [26] 20.32                       | m          | m              | [26] 20.32                       | c11        | c11            |
| 11G  | Server  | [26] 20.35                       | m          | m              | [26] 20.35                       | i          | i              |
| 11H  | Session-ID  | [162]                            | c17        | c17            | [162]                            | c17        | c17            |
| 12   | Timestamp   | [26] 20.38                       | m          | m              | [26] 20.38                       | i          | i              |
| 13   | To  | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 13A  | User-Agent  | [26] 20.41                       | m          | m              | [26] 20.41                       | i          | i              |
| 14   | Via   | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 15   | Warning   | [26] 20.43                       | m          | m              | [26] 20.43                       | i          | i              |
| c1:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |                                  |            |                |                                  |            |                |
| c2:  | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |                                  |            |                |                                  |            |                |
| c3:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |                                  |            |                |                                  |            |                |
| c4:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |                                  |            |                |                                  |            |                |
| c5:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |                                  |            |                |                                  |            |                |
| c6:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c7:  | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |                                  |            |                |                                  |            |                |
| c8:  | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |                                  |            |                |                                  |            |                |
| c9:  | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |                                  |            |                |                                  |            |                |
| c10: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |                                  |            |                |                                  |            |                |
| c11: | IF A.162/11 OR A.162/12 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |                                  |            |                |                                  |            |                |
| c12: | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |                                  |            |                |                                  |            |                |
| c13: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |                                  |            |                |                                  |            |                |
| c14: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |                                  |            |                |                                  |            |                |
| c17: | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.279: Supported header fields within the REGISTER response**

| Item | Header field  | Sending          |            |                | Receiving        |            |                |
|------|---|------------------|------------|----------------|------------------|------------|----------------|
|      |   | Ref.             | RFC status | Profile status | Ref.             | RFC status | Profile status |
| 1    | Accept  | [26] 20.1        | m          | m              | [26] 20.1        | i          | i              |
| 1A   | Accept-Encoding   | [26] 20.2        | m          | m              | [26] 20.2        | i          | i              |
| 1B   | Accept-Language   | [26] 20.3        | m          | m              | [26] 20.3        | i          | i              |
| 1C   | Accept-Resource-Priority  | [116] 3.2        | c11        | c11            | [116] 3.2        | c11        | c11            |
| 2    | Allow-Events  | [28] 7.2.2       | m          | m              | [28] 7.2.2       | c1         | c1             |
| 3    | Authentication-Info   | [26] 20.6        | m          | m              | [26] 20.6        | i          | i              |
| 5    | Contact   | [26] 20.10       | m          | m              | [26] 20.10       | i          | i              |
| 5A   | Feature-Caps  | [190]            | c16        | c16            | [190]            | c16        | c16            |
| 5B   | Flow-Timer  | [92] 11          | c12        | c12            | [92] 11          | c13        | c14            |
| 5C   | P-Associated-URI  | [52] 4.1         | c8         | c8             | [52] 4.1         | c9         | c10            |
| 6    | Path  | [35] 4.2         | c3         | c3             | [35] 4.2         | c4         | c4             |
| 7    | Security-Server   | Subclause 7.2A.7 | n/a        | c15            | Subclause 7.2A.7 | n/a        | n/a            |
| 8    | Service-Route   | [38] 5           | c5         | c5             | [38] 5           | c6         | c7             |
| 9    | Supported   | [26] 20.37       | m          | m              | [26] 20.37       | i          | i              |
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |                  |            |                |                  |            |                |
| c3:  | IF A.162/29 THEN m ELSE n/a - - Path extension support.   |                  |            |                |                  |            |                |
| c4:  | IF A.162/29 THEN i ELSE n/a - - Path extension support.   |                  |            |                |                  |            |                |
| c5:  | IF A.162/32 THEN m ELSE n/a - - Service-Route extension support.  |                  |            |                |                  |            |                |
| c6:  | IF A.162/32 THEN i ELSE n/a - - Service-Route extension support.  |                  |            |                |                  |            |                |
| c7:  | IF A.162/32 THEN (IF A.3/2 THEN m ELSE i) ELSE n/a - - Service-Route extension and P-CSCF.  |                  |            |                |                  |            |                |
| c8:  | IF A.162/36 THEN m ELSE n/a - - the P-Associated-URI extension.   |                  |            |                |                  |            |                |
| c9:  | IF A.162/36 THEN i ELSE n/a - - the P-Associated-URI extension.   |                  |            |                |                  |            |                |
| c10: | IF A.162/36 AND A.3/2 THEN m ELSE IF A.162/36 AND (A.3/3 OR A.3/9A) THEN i ELSE n/a - - the P-Associated-URI extension and P-CSCF or I-CSCF or IBCF (THIG). |                  |            |                |                  |            |                |
| c11: | IF A.162/80B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol.    |                  |            |                |                  |            |                |
| c12: | IF A.162/67 THEN m ELSE n/a - - managing client initiated transactions in SIP.  |                  |            |                |                  |            |                |
| c13: | IF A.162/67 THEN m ELSE n/a - - managing client initiated transactions in SIP, P-CSCF, I-CSCF.  |                  |            |                |                  |            |                |
| c14: | IF A.162/67 AND A.3/2 THEN m ELSE IF A.162/67 AND A.3/3 THEN i ELSE n/a - - managing client initiated transactions in SIP, P-CSCF, I-CSCF.                  |                  |            |                |                  |            |                |
| c15: | IF A.162/47A THEN m ELSE n/a - - mediasec header field parameter for marking security mechanisms related to media.  |                  |            |                |                  |            |                |
| c16: | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.   |                  |            |                |                  |            |                |



Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.279A: Supported header fields within the REGISTER response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | m          | m              | [26] 20.18 | i          | i              |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.280: Supported header fields within the REGISTER response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | c2         | c2             |
| c2:  | IF A.162/19E THEN m ELSE i - - deleting Contact headers. |            |            |                |            |            |                |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.281: Supported header fields within the REGISTER response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Proxy-Authenticate  | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 6    | Security-Server   | [48] 2     | x          | c1             | [48] 2     | n/a        | n/a            |
| 10   | WWW-Authenticate  | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |
| c1:  | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |            |            |                |            |            |                |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.282: Supported header fields within the REGISTER response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 6    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |

**Table A.283: Void**

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.284: Supported header fields within the REGISTER response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 9    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.285: Supported header fields within the REGISTER response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1 | m          | m              | [26] 20.1 | i          | i              |
| 2    | Accept-Encoding | [26] 20.2 | m          | m              | [26] 20.2 | i          | i              |
| 3    | Accept-Language | [26] 20.3 | m          | m              | [26] 20.3 | i          | i              |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.285A: Supported header fields within the REGISTER response**

| Item | Header field   | Sending   |            |                | Receiving |            |                |
|------|--|-----------|------------|----------------|-----------|------------|----------------|
|      |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority   | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.162/80B THEN m ELSE n/a - - inclusion of CANCEL, BYE, REGISTER and PUBLISH in communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.286: Supported header fields within the REGISTER response**

| Item | Header field               | Sending    |            |                | Receiving  |            |                |
|------|----------------------------|------------|------------|----------------|------------|------------|----------------|
|      |                            | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 8    | Unsupported                | [26] 20.40 | m          | m              | [26] 20.40 | c3         | c3             |
| c3:  | IF A.162/17 THEN m ELSE i. |            |            |                |            |            |                |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.286A: Supported header fields within the REGISTER response**

| Item  | Header field    | Sending |            |                | Receiving |            |                |
|---|-----------------|---------|------------|----------------|-----------|------------|----------------|
|   |                 | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3   | Security-Server | [48] 2  | c1         | c1             | [48] 2    | n/a        | n/a            |
| c1: IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |                 |         |            |                |           |            |                |

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/29 - - Additional for 423 (Interval Too Brief) response

**Table A.287: Supported header fields within the REGISTER response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Min-Expires  | [26] 20.23 | m          | m              | [26] 20.23 | i          | i              |

**Table A.288: Void**

Prerequisite A.163/19 - - REGISTER response

**Table A.289: Supported message bodies within the REGISTER response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

### A.2.2.4.13 SUBSCRIBE method

Prerequisite A.163/20 - - SUBSCRIBE request

**Table A.290: Supported header fields within the SUBSCRIBE request**

| Item | Header field                  | Sending           |            |                | Receiving         |            |                |
|------|-------------------------------|-------------------|------------|----------------|-------------------|------------|----------------|
|      |                               | Ref.              | RFC status | Profile status | Ref.              | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1         | m          | m              | [26] 20.1         | i          | i              |
| 1A   | Accept-Contact                | [56B] 9.2         | c27        | c27            | [56B] 9.2         | c27        | c28            |
| 2    | Accept-Encoding               | [26] 20.2         | m          | m              | [26] 20.2         | i          | i              |
| 3    | Accept-Language               | [26] 20.3         | m          | m              | [26] 20.3         | i          | i              |
| 3A   | Allow                         | [26] 20.5         | m          | m              | [26] 20.5         | i          | i              |
| 4    | Allow-Events                  | [28] 7.2.2        | m          | m              | [28] 7.2.2        | c1         | c1             |
| 5    | Authorization                 | [26] 20.7         | m          | m              | [26] 20.7         | i          | i              |
| 6    | Call-ID                       | [26] 20.8         | m          | m              | [26] 20.8         | m          | m              |
| 6A   | Call-Info                     | [26] 20.9         | m          | m              | [26] 20.9         | c73        | c73            |
| 6B   | Contact                       | [26] 20.10        | m          | m              | [26] 20.10        | i          | i              |
| 7    | Content-Disposition           | [26] 20.11        | m          | m              | [26] 20.11        | i          | i              |
| 8    | Content-Encoding              | [26] 20.12        | m          | m              | [26] 20.12        | i          | i              |
| 9    | Content-Language              | [26] 20.13        | m          | m              | [26] 20.13        | i          | i              |
| 10   | Content-Length                | [26] 20.14        | m          | m              | [26] 20.14        | m          | m              |
| 11   | Content-Type                  | [26] 20.15        | m          | m              | [26] 20.15        | i          | i              |
| 12   | CSeq                          | [26] 20.16        | m          | m              | [26] 20.16        | m          | m              |
| 13   | Date                          | [26] 20.17        | m          | m              | [26] 20.17        | c2         | c2             |
| 14   | Event                         | [28] 7.2.1        | m          | m              | [28] 7.2.1        | m          | m              |
| 15   | Expires                       | [26] 20.19        | m          | m              | [26] 20.19        | i          | i              |
| 15A  | Feature-Caps                  | [190]             | c74        | c74            | [190]             | c74        | c74            |
| 16   | From                          | [26] 20.20        | m          | m              | [26] 20.20        | m          | m              |
| 16A  | Geolocation                   | [89] 4.1          | c35        | c35            | [89] 4.1          | c36        | c36            |
| 16B  | Geolocation-Routing           | [89] 4.1          | c35        | c35            | [89] 4.1          | c36        | c36            |
| 16C  | History-Info                  | [66] 4.1          | c31        | c31            | [66] 4.1          | c31        | c31            |
| 16D  | Max-Breadth                   | [117] 5.8         | c47        | c47            | [117] 5.8         | c48        | c48            |
| 17   | Max-Forwards                  | [26] 20.22        | m          | m              | [26] 20.22        | m          | m              |
| 18   | MIME-Version                  | [26] 20.24        | m          | m              | [26] 20.24        | i          | i              |
| 18A  | Organization                  | [26] 20.25        | m          | m              | [26] 20.25        | c3         | c3             |
| 18B  | P-Access-Network-Info         | [52] 4.4, [234] 2 | c22        | c22            | [52] 4.4, [234] 2 | c23        | c23            |
| 18C  | P-Asserted-Identity           | [34] 9.1          | c9         | c9             | [34] 9.1          | c10        | c10            |
| 18D  | P-Asserted-Service            | [121] 4.1         | c39        | c39            | [121] 4.1         | c40        | c40            |
| 18E  | P-Called-Party-ID             | [52] 4.2          | c13        | c13            | [52] 4.2          | c14        | c15            |
| 18F  | P-Charging-Function-Addresses | [52] 4.5          | c20        | c20            | [52] 4.5          | c21        | c21            |
| 18G  | P-Charging-Vector             | [52] 4.6          | c18        | c18            | [52] 4.6          | c19        | c19            |
| 18I  | P-Preferred-Identity          | [34] 9.2          | x          | c69            | [34] 9.2          | c8         | c8             |
| 18J  | P-Preferred-Service           | [121] 4.2         | x          | x              | [121] 4.2         | c38        | c38            |
| 18K  | P-Private-Network-Indication  | [134]             | c43        | c43            | [134]             | c43        | c43            |
| 18L  | P-Profile-Key                 | [97] 5            | c33        | c33            | [97] 5            | c34        | c34            |
| 18M  | P-Served-User                 | [133] 6           | c44        | c44            | [133] 6           | c44        | c44            |
| 18N  | P-User-Database               | [82] 4            | c32        | c32            | [82] 4            | c32        | c32            |
| 18O  | P-Visited-Network-ID          | [52] 4.3          | c16        | n/a            | [52] 4.3          | c17        | n/a            |
| 18P  | Privacy                       | [33] 4.2          | c11        | c11            | [33] 4.2          | c12        | c12            |
| 19   | Proxy-Authorization           | [26] 20.28        | m          | m              | [26] 20.28        | c4         | c4             |
| 20   | Proxy-Require                 | [26] 20.29        | m          | m              | [26] 20.29        | m          | m              |
| 20A  | Reason                        | [34A] 2           | c25        | c25            | [34A] 2           | c26        | c26            |
| 21   | Record-Route                  | [26] 20.30        | m          | m              | [26] 20.30        | c7         | c7             |
| 21A  | Referred-By                   | [59] 3            | c29        | c29            | [59] 3            | c30        | c30            |
| 21B  | Reject-Contact                | [56B] 9.2         | c27        | c27            | [56B] 9.2         | c27        | c28            |
| 21C  | Request-Disposition           | [56B] 9.1         | c27        | c27            | [56B] 9.1         | c27        | c27            |
| 22   | Require                       | [26] 20.32        | m          | m              | [26] 20.32        | c5         | c5             |
| 22A  | Resource-Priority             | [116] 3.1         | c37        | c37            | [116] 3.1         | c37        | c37            |
| 23   | Route                         | [26] 20.34        | m          | m              | [26] 20.34        | m          | m              |
| 23A  | Security-Client               | [48] 2.3.1        | x          | x              | [48] 2.3.1        | c24        | c24            |
| 23B  | Security-Verify               | [48] 2.3.1        | x          | x              | [48] 2.3.1        | c24        | c24            |
| 23C  | Session-ID                    | [162]             | c70        | c70            | [162]             | c70        | c70            |
| 24   | Supported                     | [26] 20.37        | m          | m              | [26] 20.37        | c6         | c6             |
| 24A  | Target-Dialog                 | [184] 7           | c71        | c71            | [184] 7           | c72        | c72            |
| 25   | Timestamp                     | [26] 20.38        | m          | m              | [26] 20.38        | i          | i              |
| 26   | To                            | [26] 20.39        | m          | m              | [26] 20.39        | m          | m              |

|     |                 |                 |     |     |                 |     |     |
|-----|-----------------|-----------------|-----|-----|-----------------|-----|-----|
| 26A | Trigger-Consent | [125]<br>5.11.2 | c41 | c41 | [125]<br>5.11.2 | c42 | c42 |
| 27  | User-Agent      | [26] 20.41      | m   | m   | [26] 20.41      | i   | i   |
| 28  | Via             | [26] 20.42      | m   | m   | [26] 20.42      | m   | m   |

|      |   |
|------|---|
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |
| c2:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c3:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |
| c4:  | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.  |
| c5:  | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6:  | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.  |
| c7:  | IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.   |
| c8:  | IF A.162/30A OR A.162/30C THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity, act as entity passing on identity transparently independent of trust domain.   |
| c9:  | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c10: | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |
| c11: | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c12: | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c13: | IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension.   |
| c14: | IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension.   |
| c15: | IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND (A.3/3 OR A.3/9A) THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or I-CSCF or IBCF (THIG).   |
| c16: | IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension.  |
| c17: | IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response.   |
| c18: | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c19: | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c20: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c21: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c22: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c23: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c24: | IF A.162/47 OR A.162/47A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |
| c25: | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c26: | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c27: | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c28: | IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CSCF.   |
| c29: | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.  |
| c30: | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c31: | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c32: | IF A.162/60 THEN m ELSE n/a - - the P-User-Database private header extension.   |
| c33: | IF A.162/66A THEN m ELSE n/a - - making the first query to the database in order to populate the P-Profile-Key header.  |
| c34: | IF A.162/66B THEN m ELSE n/a - - using the information in the P-Profile-Key header.   |
| c35: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c36: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c37: | IF A.162/80A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.   |
| c38: | IF A.162/84A THEN m ELSE n/a - - act as authentication entity within the trust domain for asserted service.   |
| c39: | IF A.162/84 THEN m ELSE n/a - - SIP extension for the identification of services.   |
| c40: | IF A.162/84 OR A.162/30B THEN m ELSE i - - SIP extension for the identification of services or subsequent entity within trust network that can route outside the trust network.   |

|       |  |
|-------|--|
| c41:  | IF A.162/85 THEN m ELSE n/a - - a framework for consent-based communications in SIP.   |
| c42:  | IF A.162/85 THEN i ELSE n/a - - a framework for consent-based communications in SIP.   |
| c43:  | IF A.162/87 THEN m ELSE n/a - - the SIP P-Private-Network-Indication private-header (P-Header).  |
| c44:  | IF A.162/88 THEN m ELSE n/a - - the SIP P-Served-User private header.  |
| c47:  | IF A.162/81 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.  |
| c48:  | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, forking of initial requests. |
| c69:  | IF A.162/30C THEN m ELSE x - - act as entity passing on identity transparently independent of trust domain.  |
| c70:  | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.  |
| c71:  | IF A.162/109 THEN m ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.   |
| c72:  | IF A.162/109 THEN i ELSE n/a - - request authorization through dialog Identification in the session initiation protocol.   |
| c73:  | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header field.   |
| c74:  | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.  |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.   |

Prerequisite A.163/20 - - SUBSCRIBE request

**Table A.291: Supported message bodies within the SUBSCRIBE request**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/1 - - Additional for 100 (Trying) response

**Table A.291A: Supported header fields within the SUBSCRIBE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID   | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length  | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq  | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date  | [26] 20.17 | c1         | c1             | [26] 20.17 | c2         | c2             |
| 5    | From  | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
| 6    | To  | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies. |            |            |                |            |            |                |
| c2:  | IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.   |            |            |                |            |            |                |



Prerequisite A.163/21 - - SUBSCRIBE response for all remaining status-codes

**Table A.292: Supported header fields within the SUBSCRIBE response**

| Item | Header field                  | Sending                          |            |                | Receiving                        |            |                |
|------|-------------------------------|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |                               | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow                         | [26] 20.5                        | m          | m              | [26] 20.5                        | i          | i              |
| 1    | Call-ID                       | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 1A   | Call-Info                     | [26] 20.9                        | m          | m              | [26] 20.9                        | c23        | c23            |
| 2    | Content-Disposition           | [26] 20.11                       | m          | m              | [26] 20.11                       | i          | i              |
| 3    | Content-Encoding              | [26] 20.12                       | m          | m              | [26] 20.12                       | i          | i              |
| 4    | Content-Language              | [26] 20.13                       | m          | m              | [26] 20.13                       | i          | i              |
| 5    | Content-Length                | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6    | Content-Type                  | [26] 20.15                       | m          | m              | [26] 20.15                       | i          | i              |
| 7    | CSeq                          | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8    | Date                          | [26] 20.17                       | m          | m              | [26] 20.17                       | c1         | c1             |
| 9    | From                          | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A   | Geolocation-Error             | [89] 4.3                         | c20        | c20            | [89] 4.3                         | c21        | c21            |
| 9B   | History-Info                  | [66] 4.1                         | c15        | c15            | [66] 4.1                         | c15        | c15            |
| 10   | MIME-Version                  | [26] 20.24                       | m          | m              | [26] 20.24                       | i          | i              |
| 10A  | Organization                  | [26] 20.25                       | m          | m              | [26] 20.25                       | c2         | c2             |
| 10B  | P-Access-Network-Info         | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c12        | c12            | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c13        | c13            |
| 10C  | P-Asserted-Identity           | [34] 9.1                         | c4         | c4             | [34] 9.1                         | c5         | c5             |
| 10D  | P-Charging-Function-Addresses | [52] 4.5,<br>[52A] 4             | c10        | c10            | [52] 4.5,<br>[52A] 4             | c11        | c11            |
| 10E  | P-Charging-Vector             | [52] 4.6,<br>[52A] 4             | c8         | c8             | [52] 4.6,<br>[52A] 4             | c9         | c9             |
| 10G  | P-Preferred-Identity          | [34] 9.2                         | x          | x              | [34] 9.2                         | c3         | n/a            |
| 10H  | Privacy                       | [33] 4.2                         | c6         | c6             | [33] 4.2                         | c7         | c7             |
| 10I  | Require                       | [26] 20.32                       | m          | m              | [26] 20.32                       | c14        | c14            |
| 10J  | Server                        | [26] 20.35                       | m          | m              | [26] 20.35                       | i          | i              |
| 10K  | Session-ID                    | [162]                            | c22        | c22            | [162]                            | c22        | c22            |
| 11   | Timestamp                     | [26] 20.38                       | m          | m              | [26] 20.38                       | i          | i              |
| 12   | To                            | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 12A  | User-Agent                    | [26] 20.41                       | m          | m              | [26] 20.41                       | i          | i              |
| 13   | Via                           | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 14   | Warning                       | [26] 20.43                       | m          | m              | [26] 20.43                       | i          | i              |

|      |   |
|------|---|
| c1:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c2:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |
| c3:  | IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.   |
| c4:  | IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.  |
| c5:  | IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.                               |
| c6:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c7:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c8:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c9:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c10: | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c11: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c12: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c13: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c14: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c15: | IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.  |
| c16: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c17: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c20: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c21: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c22: | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |
| c23: | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header field.  |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.293: Supported header fields within the SUBSCRIBE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Accept-Resource-Priority  | [116] 3.2  | c4         | c4             | [116] 3.2  | c4         | c4             |
| 0B   | Allow-Events  | [28] 7.2.2 | m          | m              | [28] 7.2.2 | i          | i              |
| 1    | Authentication-Info   | [26] 20.6  | m          | m              | [26] 20.6  | i          | i              |
| 1A   | Contact   | [26] 20.10 | m          | m              | [26] 20.10 | i          | i              |
| 2    | Expires   | [26] 20.19 | m          | m              | [26] 20.19 | i          | i              |
| 2A   | Feature-Caps  | [190]      | c6         | c6             | [190]      | c6         | c6             |
| 3    | Record-Route  | [26] 20.30 | m          | m              | [26] 20.30 | c3         | c3             |
| 6    | Supported   | [26] 20.37 | m          | m              | [26] 20.37 | i          | i              |
| c3:  | IF A.162/15 THEN m ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routing. |            |            |                |            |            |                |
| c4:  | IF A.162/80A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol.     |            |            |                |            |            |                |
| c6:  | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.   |            |            |                |            |            |                |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.293A: Supported header fields within the SUBSCRIBE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | m          | m              | [26] 20.18 | i          | i              |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

**Table A.294: Supported header fields within the SUBSCRIBE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | c1         | c1             |
| c1:  | IF A.162/19E THEN m ELSE i - - deleting Contact headers. |            |            |                |            |            |                |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.295: Supported header fields within the SUBSCRIBE response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 8    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480 (Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.296: Supported header fields within the SUBSCRIBE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |

**Table A.297: Void**

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.298: Supported header fields within the SUBSCRIBE response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 6    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.299: Supported header fields within the SUBSCRIBE response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1 | m          | m              | [26] 20.1 | i          | i              |
| 2    | Accept-Encoding | [26] 20.2 | m          | m              | [26] 20.2 | i          | i              |
| 3    | Accept-Language | [26] 20.3 | m          | m              | [26] 20.3 | i          | i              |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.299A: Supported header fields within the SUBSCRIBE response**

| Item | Header field  | Sending   |            |                | Receiving |            |                |
|------|---|-----------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept-Resource-Priority  | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1:  | IF A.162/80A THEN m ELSE n/a - - inclusion of MESSAGE, SUBSCRIBE, NOTIFY in communications resource priority for the session initiation protocol. |           |            |                |           |            |                |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.300: Supported header fields within the SUBSCRIBE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | c3         | c3             |
| c3:  | IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. |            |            |                |            |            |                |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.300A: Supported header fields within the SUBSCRIBE response**

| Item | Header field  | Sending |            |                | Receiving |            |                |
|------|---|---------|------------|----------------|-----------|------------|----------------|
|      |   | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3    | Security-Server   | [48] 2  | c1         | c1             | [48] 2    | n/a        | n/a            |
| c1:  | IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |         |            |                |           |            |                |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/29 - - Additional for 423 (Interval Too Brief) response

**Table A.301: Supported header fields within the SUBSCRIBE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Min-Expires  | [26] 20.23 | m          | m              | [26] 20.23 | i          | i              |

**Table A.302: Void**

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/29H - - Additional for 470 (Consent Needed) response

**Table A.302A: Supported header fields within the SUBSCRIBE response**

| Item | Header field       | Sending        |            |                | Receiving      |            |                |
|------|--------------------|----------------|------------|----------------|----------------|------------|----------------|
|      |                    | Ref.           | RFC status | Profile status | Ref.           | RFC status | Profile status |
| 1    | Permission-Missing | [125]<br>5.9.3 | m          | m              | [125]<br>5.9.3 | m          | m              |

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/39 - - Additional for 489 (Bad Event) response

**Table A.303: Supported header fields within the SUBSCRIBE response**

| Item   | Header field | Sending    |            |                | Receiving  |            |                |
|--|--------------|------------|------------|----------------|------------|------------|----------------|
|  |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1  | Allow-Events | [28] 7.2.2 | m          | m              | [28] 7.2.2 | c1         | c1             |
| c1: IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.   |              |            |            |                |            |            |                |
| NOTE: c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY. |              |            |            |                |            |            |                |

**Table A.303A: Void**

Prerequisite A.163/21 - - SUBSCRIBE response

**Table A.304: Supported message bodies within the SUBSCRIBE response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

#### A.2.2.4.14 UPDATE method

Prerequisite A.163/22 - - UPDATE request

**Table A.305: Supported header fields within the UPDATE request**

| Item | Header field                  | Sending              |            |                | Receiving            |            |                |
|------|-------------------------------|----------------------|------------|----------------|----------------------|------------|----------------|
|      |                               | Ref.                 | RFC status | Profile status | Ref.                 | RFC status | Profile status |
| 1    | Accept                        | [26] 20.1            | m          | m              | [26] 20.1            | i          | i              |
| 1A   | Accept-Contact                | [56B] 9.2            | c21        | c21            | [56B] 9.2            | c22        | c22            |
| 2    | Accept-Encoding               | [26] 20.2            | m          | m              | [26] 20.2            | i          | i              |
| 3    | Accept-Language               | [26] 20.3            | m          | m              | [26] 20.3            | i          | i              |
| 4    | Allow                         | [26] 20.5            | m          | m              | [26] 20.5            | i          | i              |
| 5    | Allow-Events                  | [28] 7.2.2           | m          | m              | [28] 7.2.2           | c1         | c1             |
| 6    | Authorization                 | [26] 20.7            | m          | m              | [26] 20.7            | i          | i              |
| 7    | Call-ID                       | [26] 20.8            | m          | m              | [26] 20.8            | m          | m              |
| 8    | Call-Info                     | [26] 20.9            | m          | m              | [26] 20.9            | c8         | c8             |
| 9    | Contact                       | [26] 20.10           | m          | m              | [26] 20.10           | i          | i              |
| 10   | Content-Disposition           | [26] 20.11           | m          | m              | [26] 20.11           | c4         | c4             |
| 11   | Content-Encoding              | [26] 20.12           | m          | m              | [26] 20.12           | c4         | c4             |
| 12   | Content-Language              | [26] 20.13           | m          | m              | [26] 20.13           | c4         | c4             |
| 13   | Content-Length                | [26] 20.14           | m          | m              | [26] 20.14           | m          | m              |
| 14   | Content-Type                  | [26] 20.15           | m          | m              | [26] 20.15           | c4         | c4             |
| 15   | CSeq                          | [26] 20.16           | m          | m              | [26] 20.16           | m          | m              |
| 16   | Date                          | [26] 20.17           | m          | m              | [26] 20.17           | c2         | c2             |
| 16A  | Feature-Caps                  | [190]                | c49        | c49            | [190]                | c49        | c49            |
| 17   | From                          | [26] 20.20           | m          | m              | [26] 20.20           | m          | m              |
| 17A  | Geolocation                   | [89] 4.1             | c26        | c26            | [89] 4.1             | c27        | c27            |
| 17B  | Geolocation-Routing           | [89] 4.1             | c26        | c26            | [89] 4.1             | c27        | c27            |
| 17C  | Max-Breadth                   | [117] 5.8            | c32        | c32            | [117] 5.8            | c33        | c33            |
| 18   | Max-Forwards                  | [26] 20.22           | m          | m              | [26] 20.22           | m          | m              |
| 19   | MIME-Version                  | [26] 20.24           | m          | m              | [26] 20.24           | i          | c4             |
| 19A  | Min-SE                        | [58] 5               | c23        | c23            | [58] 5               | c23        | c23            |
| 20   | Organization                  | [26] 20.25           | m          | m              | [26] 20.25           | c3         | c3             |
| 20A  | P-Access-Network-Info         | [52] 4.4,<br>[234] 2 | c16        | c16            | [52] 4.4,<br>[234] 2 | c17        | c17            |
| 20B  | P-Charging-Function-Addresses | [52] 4.5             | c14        | c14            | [52] 4.5             | c15        | c15            |
| 20C  | P-Charging-Vector             | [52] 4.6             | c12        | c12            | [52] 4.6             | c13        | c13            |
| 20E  | P-Early-Media                 | [109] 8              | o          | c28            | [109] 8              | o          | c29            |
| 20F  | Privacy                       | [33] 4.2             | c10        | c10            | [33] 4.2             | c11        | c11            |
| 21   | Proxy-Authorization           | [26] 20.28           | m          | m              | [26] 20.28           | c9         | c9             |
| 22   | Proxy-Require                 | [26] 20.29           | m          | m              | [26] 20.29           | m          | m              |
| 22A  | Reason                        | [34A] 2              | c19        | c19            | [34A] 2              | c20        | c20            |
| 23   | Record-Route                  | [26] 20.30           | m          | m              | [26] 20.30           | c7         | c7             |
| 23A  | Recv-Info                     | [25] 5.2.3           | c34        | c34            | [25] 5.2.3           | c35        | c35            |
| 23B  | Referred-By                   | [59] 3               | c24        | c24            | [59] 3               | c25        | c25            |
| 23C  | Reject-Contact                | [56B] 9.2            | c21        | c21            | [56B] 9.2            | c22        | c22            |
| 23D  | Request-Disposition           | [56B] 9.1            | c21        | c21            | [56B] 9.1            | c22        | c22            |
| 24   | Require                       | [26] 20.32           | m          | m              | [26] 20.32           | c5         | c5             |
| 24A  | Resource-Priority             | [116] 3.1            | c47        | c47            | [116] 3.1            | c47        | c47            |
| 25   | Route                         | [26] 20.34           | m          | m              | [26] 20.34           | m          | m              |
| 25A  | Security-Client               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c18        | c18            |
| 25B  | Security-Verify               | [48] 2.3.1           | x          | x              | [48] 2.3.1           | c18        | c18            |
| 25C  | Session-Expires               | [58] 4               | c23        | c23            | [58] 4               | c23        | c23            |
| 25D  | Session-ID                    | [162]                | c48        | c48            | [162]                | c48        | c48            |
| 26   | Supported                     | [26] 20.37           | m          | m              | [26] 20.37           | c6         | c6             |
| 27   | Timestamp                     | [26] 20.38           | m          | m              | [26] 20.38           | i          | i              |
| 28   | To                            | [26] 20.39           | m          | m              | [26] 20.39           | m          | m              |
| 29   | User-Agent                    | [26] 20.41           | m          | m              | [26] 20.41           | i          | i              |
| 30   | Via                           | [26] 20.42           | m          | m              | [26] 20.42           | m          | m              |



|       |   |
|-------|---|
| c1:   | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |
| c2:   | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |
| c3:   | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |
| c4:   | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.   |
| c5:   | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |
| c6:   | IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.  |
| c7:   | IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.   |
| c8:   | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |
| c9:   | IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.  |
| c10:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |
| c11:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |
| c12:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |
| c13:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |
| c14:  | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |
| c15:  | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |
| c16:  | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c17:  | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |
| c18:  | IF A.162/47 OR A.162/47A THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol or mediasec header field parameter for marking security mechanisms related to media.  |
| c19:  | IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c20:  | IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.  |
| c21:  | IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.   |
| c22:  | IF A.162/50 THEN i ELSE n/a - - caller preferences for the session initiation protocol.   |
| c23:  | IF A.162/52 THEN m ELSE n/a - - the SIP session timer.  |
| c24:  | IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.  |
| c25:  | IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.  |
| c26:  | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |
| c27:  | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |
| c28:  | IF A.162/76 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.  |
| c29:  | IF A.162/76 THEN (IF A.3/2 THEN m ELSE i) ELSE n/a - - P-CSCF, using the information in the P-Early-Media header.   |
| c32:  | IF A.162/81 THEN m ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies.   |
| c33:  | IF A.162/81 AND A.162/6 THEN m ELSE IF A.162/81 AND NOT A.162/6 THEN i ELSE n/a - - addressing an amplification vulnerability in session initiation protocol forking proxies, forking of initial requests.  |
| c34:  | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |
| c35:  | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |
| c47:  | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.   |
| c48:  | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |
| c49:  | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.   |
| NOTE: | c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.  |

Prerequisite A.163/22 - - UPDATE request

**Table A.306: Supported message bodies within the UPDATE request**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/1 - - Additional for 100 (Trying) response

**Table A.306A: Supported header fields within the UPDATE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Call-ID   | [26] 20.8  | m          | m              | [26] 20.8  | m          | m              |
| 2    | Content-Length  | [26] 20.14 | m          | m              | [26] 20.14 | m          | m              |
| 3    | CSeq  | [26] 20.16 | m          | m              | [26] 20.16 | m          | m              |
| 4    | Date  | [26] 20.17 | c1         | c1             | [26] 20.17 | c2         | c2             |
| 5    | From  | [26] 20.20 | m          | m              | [26] 20.20 | m          | m              |
|      |   |            |            |                |            |            |                |
| 6    | To  | [26] 20.39 | m          | m              | [26] 20.39 | m          | m              |
| 7    | Via   | [26] 20.42 | m          | m              | [26] 20.42 | m          | m              |
| c1:  | IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies. |            |            |                |            |            |                |
| c2:  | IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.   |            |            |                |            |            |                |

Prerequisite A.163/22 - - UPDATE response for all remaining status-codes

**Table A.307: Supported header fields within the UPDATE response**

| Item | Header field  | Sending                          |            |                | Receiving                        |            |                |
|------|---|----------------------------------|------------|----------------|----------------------------------|------------|----------------|
|      |   | Ref.                             | RFC status | Profile status | Ref.                             | RFC status | Profile status |
| 0A   | Allow   | [26] 20.5                        | m          | m              | [26] 20.5                        | i          | i              |
| 1    | Call-ID   | [26] 20.8                        | m          | m              | [26] 20.8                        | m          | m              |
| 1A   | Call-Info   | [26] 20.9                        | m          | m              | [26] 20.9                        | c4         | c4             |
| 1B   | Contact   | [26] 20.10                       | m          | m              | [26] 20.10                       | i          | i              |
| 2    | Content-Disposition   | [26] 20.11                       | m          | m              | [26] 20.11                       | i          | c3             |
| 3    | Content-Encoding  | [26] 20.12                       | m          | m              | [26] 20.12                       | i          | c3             |
| 4    | Content-Language  | [26] 20.13                       | m          | m              | [26] 20.13                       | i          | c3             |
| 5    | Content-Length  | [26] 20.14                       | m          | m              | [26] 20.14                       | m          | m              |
| 6    | Content-Type  | [26] 20.15                       | m          | m              | [26] 20.15                       | i          | c3             |
| 7    | CSeq  | [26] 20.16                       | m          | m              | [26] 20.16                       | m          | m              |
| 8    | Date  | [26] 20.17                       | m          | m              | [26] 20.17                       | c1         | c1             |
| 9    | From  | [26] 20.20                       | m          | m              | [26] 20.20                       | m          | m              |
| 9A   | Geolocation-Error   | [89] 4.3                         | c14        | c14            | [89] 4.3                         | c15        | c15            |
| 10   | MIME-Version  | [26] 20.24                       | m          | m              | [26] 20.24                       | i          | c3             |
| 10A  | Organization  | [26] 20.25                       | m          | m              | [26] 20.25                       | c2         | c2             |
| 10B  | P-Access-Network-Info   | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c11        | c11            | [52] 4.4,<br>[52A] 4,<br>[234] 2 | c12        | c12            |
| 10C  | P-Charging-Function-Addresses   | [52] 4.5,<br>[52A] 4             | c9         | c9             | [52] 4.5,<br>[52A] 4             | c10        | c10            |
| 10D  | P-Charging-Vector   | [52] 4.6,<br>[52A] 4             | c7         | n/a            | [52] 4.6,<br>[52A] 4             | c8         | n/a            |
| 10F  | Privacy   | [33] 4.2                         | c5         | c5             | [33] 4.2                         | c6         | c6             |
| 10G  | Recv-Info   | [25] 5.2.3                       | c18        | c18            | [25] 5.2.3                       | c19        | c19            |
| 10H  | Require   | [26] 20.32                       | m          | m              | [26] 20.32                       | c13        | c13            |
| 10I  | Server  | [26] 20.35                       | m          | m              | [26] 20.35                       | i          | i              |
| 10J  | Session-ID  | [162]                            | c20        | c20            | [162]                            | c20        | c20            |
| 11   | Timestamp   | [26] 20.38                       | m          | m              | [26] 20.38                       | i          | i              |
| 12   | To  | [26] 20.39                       | m          | m              | [26] 20.39                       | m          | m              |
| 12A  | User-Agent  | [26] 20.41                       | m          | m              | [26] 20.41                       | i          | i              |
| 13   | Via   | [26] 20.42                       | m          | m              | [26] 20.42                       | m          | m              |
| 14   | Warning   | [26] 20.43                       | m          | m              | [26] 20.43                       | i          | i              |
| c1:  | IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.   |                                  |            |                |                                  |            |                |
| c2:  | IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.   |                                  |            |                |                                  |            |                |
| c3:  | IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.   |                                  |            |                |                                  |            |                |
| c4:  | IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.  |                                  |            |                |                                  |            |                |
| c5:  | IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).  |                                  |            |                |                                  |            |                |
| c6:  | IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.  |                                  |            |                |                                  |            |                |
| c7:  | IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.   |                                  |            |                |                                  |            |                |
| c8:  | IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.  |                                  |            |                |                                  |            |                |
| c9:  | IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.   |                                  |            |                |                                  |            |                |
| c10: | IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.                                   |                                  |            |                |                                  |            |                |
| c11: | IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |                                  |            |                |                                  |            |                |
| c12: | IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.                                      |                                  |            |                |                                  |            |                |
| c13: | IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER. |                                  |            |                |                                  |            |                |
| c14: | IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.  |                                  |            |                |                                  |            |                |
| c15: | IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.   |                                  |            |                |                                  |            |                |
| c18: | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |                                  |            |                |                                  |            |                |
| c19: | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |                                  |            |                |                                  |            |                |
| c20: | IF A.162/101 THEN m ELSE n/a - - the Session-ID header.   |                                  |            |                |                                  |            |                |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/102 - - Additional for 2xx response

**Table A.308: Supported header fields within the UPDATE response**

| Item | Header field  | Sending    |            |                | Receiving  |            |                |
|------|---|------------|------------|----------------|------------|------------|----------------|
|      |   | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 0A   | Accept  | [26] 20.1  | m          | m              | [26] 20.1  | i          | i              |
| 0B   | Accept-Encoding   | [26] 20.2  | m          | m              | [26] 20.2  | i          | i              |
| 0C   | Accept-Language   | [26] 20.3  | m          | m              | [26] 20.3  | i          | i              |
| 0D   | Accept-Resource-Priority  | [116] 3.2  | c12        | c12            | [116] 3.2  | c12        | c12            |
| 1    | Allow-Events  | [28] 7.2.2 | m          | m              | [28] 7.2.2 | c1         | c1             |
| 2    | Authentication-Info   | [26] 20.6  | m          | m              | [26] 20.6  | i          | i              |
| 3    | Contact   | [26] 20.10 | m          | m              | [26] 20.10 | i          | i              |
| 3A   | Feature-Caps  | [190]      | c14        | c14            | [190]      | c14        | c14            |
| 3B   | P-Early-Media   | [109] 8    | o          | c10            | [109] 8    | o          | c11            |
| 3D   | Recv-Info   | [25] 5.2.3 | c5         | c5             | [25] 5.2.3 | c6         | c6             |
| 4    | Session-Expires   | [58] 4     | c4         | c4             | [58] 4     | c4         | c4             |
| 6    | Supported   | [26] 20.37 | m          | m              | [26] 20.37 | i          | i              |
| c1:  | IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.  |            |            |                |            |            |                |
| c3:  | IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routing. |            |            |                |            |            |                |
| c4:  | IF A.162/52 THEN m ELSE n/a - - the SIP session timer.  |            |            |                |            |            |                |
| c5:  | IF A.162/20 THEN m ELSE n/a - - SIP INFO method and package framework.  |            |            |                |            |            |                |
| c6:  | IF A.162/20 THEN i ELSE n/a - - SIP INFO method and package framework.  |            |            |                |            |            |                |
| c10: | IF A.162/76 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.                                      |            |            |                |            |            |                |
| c11: | IF A.162/76 THEN (IF A.3/2 THEN m ELSE i) ELSE n/a - - P-CSCF, using the information in the P-Early-Media header.                                     |            |            |                |            |            |                |
| c12: | IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol.   |            |            |                |            |            |                |
| c14: | IF A.162/110 THEN m ELSE n/a - - indication of features supported by proxy.   |            |            |                |            |            |                |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

**Table A.308A: Supported header fields within the UPDATE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 1    | Error-Info   | [26] 20.18 | m          | m              | [26] 20.18 | i          | i              |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/103 or A.164/35 - - Additional for 3xx, 485 (Ambiguous) response

**Table A.309: Supported header fields within the UPDATE response**

| Item | Header field   | Sending    |            |                | Receiving  |            |                |
|------|--|------------|------------|----------------|------------|------------|----------------|
|      |  | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 2    | Contact  | [26] 20.10 | m          | m              | [26] 20.10 | c1         | c1             |
| c1:  | IF A.162/19E THEN m ELSE i - - deleting Contact headers. |            |            |                |            |            |                |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

**Table A.309A: Supported header fields within the UPDATE response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 3    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 6    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

**Table A.310: Supported header fields within the UPDATE response**

| Item | Header field | Sending    |            |                | Receiving  |            |                |
|------|--------------|------------|------------|----------------|------------|------------|----------------|
|      |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 5    | Retry-After  | [26] 20.33 | m          | m              | [26] 20.33 | i          | i              |

**Table A.311: Void**

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

**Table A.312: Supported header fields within the UPDATE response**

| Item | Header field       | Sending    |            |                | Receiving  |            |                |
|------|--------------------|------------|------------|----------------|------------|------------|----------------|
|      |                    | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 4    | Proxy-Authenticate | [26] 20.27 | m          | m              | [26] 20.27 | m          | m              |
| 8    | WWW-Authenticate   | [26] 20.44 | m          | m              | [26] 20.44 | i          | i              |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

**Table A.313: Supported header fields within the UPDATE response**

| Item | Header field    | Sending   |            |                | Receiving |            |                |
|------|-----------------|-----------|------------|----------------|-----------|------------|----------------|
|      |                 | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    | Accept          | [26] 20.1 | m          | m              | [26] 20.1 | i          | i              |
| 2    | Accept-Encoding | [26] 20.2 | m          | m              | [26] 20.2 | i          | i              |
| 3    | Accept-Language | [26] 20.3 | m          | m              | [26] 20.3 | i          | i              |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/26A - - Additional for 417 (Unknown Resource-Priority) response

**Table A.313A: Supported header fields within the UPDATE response**

| Item  | Header field             | Sending   |            |                | Receiving |            |                |
|---|--------------------------|-----------|------------|----------------|-----------|------------|----------------|
|   |                          | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1   | Accept-Resource-Priority | [116] 3.2 | c1         | c1             | [116] 3.2 | c1         | c1             |
| c1: IF A.162/80 THEN m ELSE n/a - - communications resource priority for the session initiation protocol. |                          |           |            |                |           |            |                |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

**Table A.314: Supported header fields within the UPDATE response**

| Item   | Header field | Sending    |            |                | Receiving  |            |                |
|--|--------------|------------|------------|----------------|------------|------------|----------------|
|  |              | Ref.       | RFC status | Profile status | Ref.       | RFC status | Profile status |
| 7  | Unsupported  | [26] 20.40 | m          | m              | [26] 20.40 | c3         | c3             |
| c3: IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER. |              |            |            |                |            |            |                |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

**Table A.314A: Supported header fields within the UPDATE response**

| Item  | Header field    | Sending |            |                | Receiving |            |                |
|---|-----------------|---------|------------|----------------|-----------|------------|----------------|
|   |                 | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 3   | Security-Server | [48] 2  | c1         | c1             | [48] 2    | n/a        | n/a            |
| c1: IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. |                 |         |            |                |           |            |                |

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/28A - - Additional for 422 (Session Interval Too Small) response

**Table A.314B: Supported header fields within the UPDATE response**

| Item   | Header field | Sending |            |                | Receiving |            |                |
|--|--------------|---------|------------|----------------|-----------|------------|----------------|
|  |              | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1  | Min-SE       | [58] 5  | c1         | c1             | [58] 5    | c1         | c1             |
| c1: IF A.162/52 THEN m ELSE n/a - - the SIP session timer. |              |         |            |                |           |            |                |

**Table A.315: Void**

Prerequisite A.163/23 - - UPDATE response

**Table A.316: Supported message bodies within the UPDATE response**

| Item | Header | Sending |            |                | Receiving |            |                |
|------|--------|---------|------------|----------------|-----------|------------|----------------|
|      |        | Ref.    | RFC status | Profile status | Ref.      | RFC status | Profile status |
| 1    |        |         |            |                |           |            |                |

## A.3 Profile definition for the Session Description Protocol as used in the present document

### A.3.1 Introduction

Void.

### A.3.2 User agent role

This subclause contains the ICS proforma tables related to the user agent role. They need to be completed only for UA implementations.

Prerequisite: A.2/1 -- user agent role



### A.3.2.1 Major capabilities

**Table A.317: Major capabilities**

| Item | Does the implementation support  | Reference | RFC status | Profile status |
|------|--|-----------|------------|----------------|
|      | <b>Capabilities within main protocol</b>   |           |            |                |
|      | <b>Extensions</b>  |           |            |                |
| 22   | integration of resource management and SIP?  | [30] [64] | o          | c14            |
| 23   | grouping of media lines?   | [53]      | c3         | c3             |
| 24   | mapping of media streams to resource reservation flows?  | [54]      | o          | c1             |
| 25   | SDP bandwidth modifiers for RTCP bandwidth?  | [56]      | o          | o (NOTE 1)     |
| 26   | TCP-based media transport in the session description protocol?   | [83]      | o          | c2             |
| 27   | interactive connectivity establishment?  | [99]      | o          | c4             |
| 28   | session description protocol format for binary floor control protocol streams?   | [108]     | o          | o              |
| 29   | extended RTP profile for real-time transport control protocol (RTCP)-based feedback (RTP/AVPF)?  | [135]     | o          | c5             |
| 30   | SDP capability negotiation?  | [137]     | o          | c6             |
| 31   | Session Description Protocol (SDP) extension for setting up audio media streams over circuit-switched bearers in the Public Switched Telephone Network (PSTN)? | [155]     | o          | c7             |
| 32   | miscellaneous capabilities negotiation in the Session Description Protocol (SDP)?  | [156]     | o          | c7             |
| 33   | transport independent bandwidth modifier for the Session Description Protocol?   | [152]     | o          | c8             |
| 34   | Secure Real-time Transport Protocol (SRTP)?  | [169]     | o          | c15            |
| 35   | MIKEY-TICKET?  | [170]     | o          | c10            |
| 36   | SDES?  | [168]     | o          | c9             |
| 37   | end-to-access-edge media security using SDES?  | 7.5.2     | n/a        | c16            |
| 38   | SDP media capabilities negotiation?  | [172]     | o          | c12            |
| 39   | Transcoding Services Invocation in the Session Initiation Protocol (SIP) Using Third Party Call Control (3pcc)?  | [166]     | o          | c13            |
| 40   | Message Session Relay Protocol?  | [178]     | o          | c17            |
| 41   | a SDP offer/answer mechanism to enable file transfer?  | [185]     | o          | o              |
| 42   | optimal media routing  | [11D]     | n/a        | c18            |
| 43   | ECN for RTP over UDP   | [188]     | o          | c19            |
| 44   | T.38 FAX?  | [202]     | n/a        | c20            |
| 45   | support for reduced-size RTCP?   | [204]     | o          | o              |
| 46   | RTCP extended reports?   | [205]     | o          | o              |
| 47   | maximum receive SDU size?  | [9B]      | o          | o              |
| 48   | the SDP content attribute  | [206]     | o          | c21            |

|         |   |
|---------|---|
| c1:     | IF A.3/1 THEN m ELSE n/a - - UE role.   |
| c2:     | IF A.3/9B AND A.3/13B THEN m ELSE IF A.3/1 OR A.3/6 OR A.3/7 THEN o ELSE n/a - - IBCF (IMS-ALG), application gateway function (IMS-ALG), UE, MGCF, AS.  |
| c3:     | IF A.317/24 THEN m ELSE o - - mapping of media streams to resource reservation flows.   |
| c4:     | IF A.3/9B OR A.3/13B THEN m ELSE IF A.3/1 OR A.3/6 THEN o ELSE n/a - - IBCF (IMS-ALG), application gateway function (IMS-ALG), UE, MGCF.  |
| c5:     | IF A.3A/50 OR A.3A/50A OR A.3/6 OR A.3/9B OR A.3A/89 THEN m ELSE o - - multimedia telephony service participant, multimedia telephony service application server, MGCF, IBCF (IMS-ALG), ATCF (UA).  |
| c6:     | IF A.3A/50 OR A.3A/50A OR A.3/6 OR A.3/9B OR A.3/13B OR A.3A/89 THEN m ELSE o - - multimedia telephony service participant, multimedia telephony service application server, MGCF, IBCF (IMS-ALG), application gateway function (IMS-ALG), ATCF (UA).                                     |
| c7:     | IF A.3A/82 OR A.3A/83 THEN m ELSE o - - ICS user agent, SCC application server.   |
| c8:     | IF A.317/25 AND (A.3/1 OR A.3/6 OR A.3A/89) THEN o ELSE n/a - - SDP bandwidth modifiers for RTCP bandwidth, UE, MGCF, ATCF (UA).  |
| c9:     | IF A.3D/30 OR A.3D/20 THEN m ELSE n/a - - end-to-access-edge media security using SDES, end-to-end media security using SDES.   |
| c10:    | IF A.3D/21 THEN m ELSE n/a - - end-to-end media security using KMS.   |
| c12:    | IF A.3A/82 OR A.3A/83 THEN m ELSE o - - ICS user agent, SCC application server.   |
| c13:    | IF IF A.3/7D OR A.3/8 THEN o ELSE n/a - - AS performing 3rd party call control or MRFC.   |
| c14:    | IF A.4/2C THEN m ELSE o - - initiating a session which require local and/or remote resource reservation.  |
| c15:    | IF A.3D/20 OR A.3D/21 OR A.3D/30 THEN m ELSE n/a - - end-to-end media security using SDES, end-to-end media security using KMS, end-to-access-edge media security using SDES.   |
| c16:    | IF A.3D/30 THEN m ELSE n/a - - end-to-access-edge media security using SDES.  |
| c17:    | IF A.3A/33B OR A.3A/34 THEN m ELSE IF A.3A/8 OR A.3A/9 THEN o ELSE n/a - - session-mode messaging participant, session-mode messaging intermediate node, IBCF, MRFC.  |
| c18:    | IF A.3/2A OR A.3/6 OR A.3/7 OR A.3/9B OR A.3A/89 OR A.3/13B THEN o ELSE n/a - - P-CSCF (IMS-ALG), MGCF, AS, IBCF (IMS-ALG), ATCF (UA), application gateway function (IMS-ALG).  |
| c19:    | IF A.3/2A OR A.3/6 OR A.3/8 OR A.3/9B OR A.3A/81 OR A.3A/89 OR A.3/13B THEN o ELSE n/a - - P-CSCF (IMS-ALG), MGCF, MRFC, IBCF (IMS-ALG), MSC Server enhanced for ICS, ATCF (UA), application gateway function (IMS-ALG).  |
| c20:    | IF A.3/1 OR A.3/6 THEN o ELSE n/a - - UE, MGCF.   |
| c21:    | IF A.3A/57 OR A.3A/58 OR A.3A/59 OR A.3A/60 OR A.3/2A OR A.3/9B THEN m ELSE o - - Customized alerting tones application server, Customized alerting tones UA client, Customized ringing signal application server, Customized ringing signal UA client, P-CSCF (IMS-ALG), IBCF (IMS-ALG). |
| NOTE 1: | For "video" and "audio" media types that utilise RTP/RTCP, if the RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556 [56], then, it shall be specified. For other media types, it may be specified.                               |

## A.3.2.2 SDP types

Table A.318: SDP types

| Item  | Type   | Sending   |            |                | Receiving |            |                |
|---|--|-----------|------------|----------------|-----------|------------|----------------|
|   |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| <b>Session level description</b>                        |  |           |            |                |           |            |                |
| 1   | v= (protocol version)  | [39] 5.1  | m          | m              | [39] 5.1  | m          | m              |
| 2   | o= (owner/creator and session identifier)  | [39] 5.2  | m          | m              | [39] 5.2  | m          | m              |
| 3   | s= (session name)  | [39] 5.3  | m          | m              | [39] 5.3  | m          | m              |
| 4   | i= (session information)   | [39] 5.4  | o          | c2             | [39] 5.4  | m          | c3             |
| 5   | u= (URI of description)  | [39] 5.5  | o          | c4             | [39] 5.5  | o          | n/a            |
| 6   | e= (email address)   | [39] 5.6  | o          | c4             | [39] 5.6  | o          | n/a            |
| 7   | p= (phone number)  | [39] 5.6  | o          | c4             | [39] 5.6  | o          | n/a            |
| 8   | c= (connection information)  | [39] 5.7  | c5         | c5             | [39] 5.7  | m          | m              |
| 9   | b= (bandwidth information)   | [39] 5.8  | o          | o<br>(NOTE 1)  | [39] 5.8  | m          | m              |
| <b>Time description (one or more per description)</b>   |  |           |            |                |           |            |                |
| 10  | t= (time the session is active)  | [39] 5.9  | m          | m              | [39] 5.9  | m          | m              |
| 11  | r= (zero or more repeat times)   | [39] 5.10 | o          | c4             | [39] 5.10 | o          | n/a            |
| <b>Session level description (continued)</b>            |  |           |            |                |           |            |                |
| 12  | z= (time zone adjustments)   | [39] 5.11 | o          | n/a            | [39] 5.11 | o          | n/a            |
| 13  | k= (encryption key)  | [39] 5.12 | x          | x              | [39] 5.12 | n/a        | n/a            |
| 14  | a= (zero or more session attribute lines)  | [39] 5.13 | o          | o              | [39] 5.13 | m          | m              |
| <b>Media description (zero or more per description)</b> |  |           |            |                |           |            |                |
| 15  | m= (media name and transport address)  | [39] 5.14 | m          | m              | [39] 5.14 | m          | m              |
| 16  | i= (media title)   | [39] 5.4  | o          | c2             | [39] 5.4  | o          | c3             |
| 17  | c= (connection information)  | [39] 5.7  | c1         | c1             | [39] 5.7  | m          | m              |
| 18  | b= (bandwidth information)   | [39] 5.8  | o          | o<br>(NOTE 1)  | [39] 5.8  | m          | m              |
| 19  | k= (encryption key)  | [39] 5.12 | x          | x              | [39] 5.12 | n/a        | n/a            |
| 20  | a= (zero or more media attribute lines)  | [39] 5.13 | o          | o              | [39] 5.13 | m          | m              |
| c1:   | IF (A.318/15 AND NOT A.318/8) THEN m ELSE IF (A.318/15 AND A.318/8) THEN o ELSE n/a -- "c=" contained in session level description and SDP contains media descriptions.  |           |            |                |           |            |                |
| c2:   | IF A.3/6 THEN x ELSE o -- MGCF.  |           |            |                |           |            |                |
| c3:   | IF A.3/6 THEN n/a ELSE m -- MGCF.  |           |            |                |           |            |                |
| c4:   | IF A.3/6 THEN x ELSE n/a -- MGCF.  |           |            |                |           |            |                |
| c5:   | IF A.318/17 THEN o ELSE m -- "c=" contained in all media description.  |           |            |                |           |            |                |
| NOTE 1:   | The UE may use b=TIAS and b=AS as described in RFC 3890 [152]. For "video" and "audio" media types that utilise RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level different than the default RTCP bandwidth as specified in RFC 3556 [56], then the UE shall include the "b=" media descriptors with the bandwidth modifiers "RS" and "RR". For other media types, the UE may include the "b=" media descriptor with the bandwidth modifiers "RS" and "RR". |           |            |                |           |            |                |

Prerequisite A.318/14 OR A.318/20 - - a= (zero or more session/media attribute lines)

**Table A.319: zero or more session / media attribute lines (a=)**

| Item | Field  | Sending                    |            |                | Receiving                  |            |                |
|------|--|----------------------------|------------|----------------|----------------------------|------------|----------------|
|      |  | Ref.                       | RFC status | Profile status | Ref.                       | RFC status | Profile status |
| 1    | category (a=cat)                                     | [39] 6                     | c8         | c8             | [39] 6                     | c9         | c9             |
| 2    | keywords (a=keywds)                                  | [39] 6                     | c8         | c8             | [39] 6                     | c9         | c9             |
| 3    | name and version of tool (a=tool)                    | [39] 6                     | c8         | c8             | [39] 6                     | c9         | c9             |
| 4    | packet time (a=ptime)                                | [39] 6                     | c10        | c10            | [39] 6                     | c11        | c11            |
| 5    | maximum packet time (a=maxptime)                     | [39] 6<br>(NOTE 1)         | c10        | c10            | [39] 6<br>(NOTE 1)         | c11        | c11            |
| 6    | receive-only mode (a=recvonly)                       | [39] 6                     | o          | o              | [39] 6                     | m          | m              |
| 7    | send and receive mode (a=sendrecv)                   | [39] 6                     | o          | o              | [39] 6                     | m          | m              |
| 8    | send-only mode (a=sendonly)                          | [39] 6                     | o          | o              | [39] 6                     | m          | m              |
| 8A   | Inactive mode (a=inactive)                           | [39] 6                     | o          | o              | [39] 6                     | m          | m              |
| 9    | whiteboard orientation (a=orient)                    | [39] 6                     | c10        | c10            | [39] 6                     | c11        | c11            |
| 10   | conference type (a=type)                             | [39] 6                     | c8         | c8             | [39] 6                     | c9         | c9             |
| 11   | character set (a=charset)                            | [39] 6                     | c8         | c8             | [39] 6                     | c9         | c9             |
| 12   | language tag (a=sdplang)                             | [39] 6                     | o          | o              | [39] 6                     | m          | m              |
| 13   | language tag (a=lang)                                | [39] 6                     | o          | o              | [39] 6                     | m          | m              |
| 14   | frame rate (a=framerate)                             | [39] 6                     | c10        | c10            | [39] 6                     | c11        | c11            |
| 15   | quality (a=quality)                                  | [39] 6                     | c10        | c10            | [39] 6                     | c11        | c11            |
| 16   | format specific parameters (a=fmtp)                  | [39] 6                     | c10        | c10            | [39] 6                     | c11        | c11            |
| 17   | rtpmap attribute (a=rtpmap)                          | [39] 6                     | c10        | c10            | [39] 6                     | c11        | c11            |
| 18   | current-status attribute (a=curr)                    | [30] 5                     | c1         | c1             | [30] 5                     | c2         | c2             |
| 19   | desired-status attribute (a=des)                     | [30] 5                     | c1         | c1             | [30] 5                     | c2         | c2             |
| 20   | confirm-status attribute (a=conf)                    | [30] 5                     | c1         | c1             | [30] 5                     | c2         | c2             |
| 21   | media stream identification attribute (a=mid)        | [53] 3                     | c3         | c3             | [53] 3                     | c4         | c4             |
| 22   | group attribute (a=group)                            | [53] 4                     | c5         | c5             | [53] 3                     | c6         | c6             |
| 23   | setup attribute (a=setup)                            | [83] 4                     | c7         | c7             | [83] 4                     | c7         | c7             |
| 24   | connection attribute (a=connection)                  | [83] 5                     | c7         | c7             | [83] 5                     | c7         | c7             |
| 25   | IP addresses (a=candidate)                           | [99]                       | c12        | c12            | [99]                       | c13        | c13            |
| 26   | floor control server determination (a=floorctrl)     | [108] 4                    | c14        | c14            | [108] 4                    | c14        | c14            |
| 27   | conference id (a=confid)                             | [108] 5                    | c14        | c14            | [108] 5                    | c14        | c14            |
| 28   | user id (a=userid)                                   | [108] 5                    | c14        | c14            | [108] 5                    | c14        | c14            |
| 29   | association between streams and floors (a=floorid)   | [108] 6                    | c14        | c14            | [108] 6                    | c14        | c14            |
| 30   | RTCP feedback capability attribute (a=rtcp-fb)       | [135] 4.2                  | c15        | c15            | [135] 4.2                  | c15        | c15            |
| 31   | extension of the rtcp-fb attribute (a=rtcp-fb)       | [136] 7.1,<br>[188] 6.2    | c15        | c15            | [136] 7.1                  | c15        | c15            |
| 32   | supported capability negotiation extensions (a=csup) | [137] 3.3.1                | c16        | c16            | [137] 3.3.1                | c16        | c16            |
| 33   | required capability negotiation extensions (a=creq)  | [137] 3.3.2                | c16        | c16            | [137] 3.3.2                | c16        | c16            |
| 34   | attribute capability (a=acap)                        | [137] 3.4.1                | c16        | c16            | [137] 3.4.1                | c16        | c16            |
| 35   | transport protocol capability (a=tcap)               | [137] 3.4.2                | c16        | c16            | [137] 3.4.2                | c16        | c16            |
| 36   | potential configuration (a=pcfg)                     | [137] 3.5.1<br>[172] 3.3.6 | c16        | c16            | [137] 3.5.1<br>[172] 3.3.6 | c16        | c16            |
| 37   | actual configuration (a=acfg)                        | [137] 3.5.2                | c16        | c16            | [137] 3.5.2                | c16        | c16            |
| 38   | connection data capability (a=ccap)                  | [156] 3.1                  | c17        | c17            | [156] 3.1                  | c18        | c18            |

|     |   |                |     |     |                |     |     |
|-----|---|----------------|-----|-----|----------------|-----|-----|
| 39  | maximum packet rate<br>(a=maxprate)                                 | [152] 6.3      | c19 | c19 | [152] 6.3      | c19 | c19 |
| 40  | crypto attribute (a=crypto)   | [168]          | c20 | c20 | [168]          | c20 | c20 |
| 41  | key management attribute<br>(a=key-mgmt)                            | [167]          | c21 | c21 | [167]          | c21 | c21 |
| 42  | 3GPP_e2ae-security-indicator<br>(a=3ge2ae)                          | 7.5.2          | c22 | c22 | 7.5.2          | c22 | c22 |
| 43  | media capability (a=rmcap)  | [172]<br>3.3.1 | c23 | c23 | [172]<br>3.3.1 | c23 | c23 |
| 43A | media capability (a=omcap)  | [172]<br>3.3.1 | c23 | c23 | [172]<br>3.3.1 | c23 | c23 |
| 44  | media format capability<br>(a=mfcap)                                | [172]<br>3.3.2 | c23 | c23 | [172]<br>3.3.2 | c23 | c23 |
| 45  | media-specific capability<br>(a=mscap)                              | [172]<br>3.3.3 | c23 | c23 | [172]<br>3.3.3 | c23 | c23 |
| 46  | latent configuration (a=lcfg)                                       | [172]<br>3.3.5 | c44 | c44 | [172]<br>3.3.5 | c44 | c44 |
| 47  | session capability (a=sescap)                                       | [172]<br>3.3.8 | c24 | c24 | [172]<br>3.3.8 | c24 | c24 |
| 48  | msrp path (a=path)  | [178]          | c25 | c25 | [178]          | c25 | c25 |
| 49  | file selector (a=file-selector)                                     | [185] 6        | c27 | c27 | [185] 6        | c28 | c28 |
| 50  | file transfer identifier (a= file-<br>transfer-id)                  | [185] 6        | c26 | c26 | [185] 6        | c28 | c28 |
| 51  | file disposition (a=file-<br>disposition)                           | [185] 6        | c26 | c26 | [185] 6        | c28 | c28 |
| 52  | file date (a=file-date)   | [185] 6        | c26 | c26 | [185] 6        | c28 | c28 |
| 53  | file icon (a=file-icon)   | [185] 6        | c26 | c26 | [185] 6        | c28 | c28 |
| 54  | file range (a=file-range)   | [185] 6        | c26 | c26 | [185] 6        | c28 | c28 |
| 55  | optimal media routeing visited<br>realm (a=visited-realm)           | 7.5.3          | c29 | c29 | 7.5.3          | c29 | c29 |
| 56  | optimal media routeing<br>secondary realm<br>(a=secondary-realm)    | 7.5.3          | c29 | c29 | 7.5.3          | c29 | c29 |
| 57  | optimal media routeing media<br>level checksum (a=omr-m-<br>cksum)  | 7.5.3          | c29 | c29 | 7.5.3          | c29 | c29 |
| 58  | optimal media routeing<br>session level checksum<br>(a=omr-s-cksum) | 7.5.3          | c29 | c29 | 7.5.3          | c29 | c29 |
| 59  | optimal media routeing codecs<br>(a=omr-codecs)                     | 7.5.3          | c29 | c29 | 7.5.3          | c29 | c29 |
| 60  | optimal media routeing media<br>attributes (a=omr-m-att)            | 7.5.3          | c29 | c29 | 7.5.3          | c29 | c29 |
| 61  | optimal media routeing<br>session attributes (a=omr-s-<br>att)      | 7.5.3          | c29 | c29 | 7.5.3          | c29 | c29 |
| 62  | optimal media routeing media<br>bandwidth (a=omr-m-bw)              | 7.5.3          | c29 | c29 | 7.5.3          | c29 | c29 |
| 63  | optimal media routeing<br>session bandwidth (a=omr-s-<br>bw)        | 7.5.3          | c29 | c29 | 7.5.3          | c29 | c29 |
| 64  | ecn-attribute (a=ecn-capable-<br>rtt)                               | [188]          | c30 | c30 | [188]          | c30 | c30 |
| 65  | T38 FAX Protocol version<br>(a=T38FaxVersion)                       | [202]          | n/a | c31 | [202]          | n/a | c31 |
| 66  | T38 FAX Maximum Bit Rate<br>(a=T38MaxBitRate)                       | [202]          | n/a | c31 | [202]          | n/a | c31 |
| 67  | T38 FAX Rate Management<br>(a=T38FaxRateManagement)                 | [202]          | n/a | c31 | [202]          | n/a | c31 |
| 68  | T38 FAX Maximum Buffer<br>Size (a=T38FaxMaxBuffer)                  | [202]          | n/a | c31 | [202]          | n/a | c31 |
| 69  | T38 FAX Maximum Datagram<br>Size<br>(a=T38FaxMaxDatagram)           | [202]          | n/a | c31 | [202]          | n/a | c31 |
| 70  | T38 FAX maximum IFP frame<br>size (a=T38FaxMaxIFP)                  | [202]          | n/a | c32 | [202]          | n/a | c32 |

|    |   |                  |     |     |                  |     |     |
|----|---|------------------|-----|-----|------------------|-----|-----|
| 71 | T38 FAX UDP Error Correction Scheme (a=T38FaxUdpEC)         | [202]            | n/a | c32 | [202]            | n/a | c32 |
| 72 | T38 FAX UDP Error Correction Depth (a=T38FaxUdpECDepth)     | [202]            | n/a | c32 | [202]            | n/a | c32 |
| 73 | T38 FAX UDP FEC Maximum Span (a=T38FaxUdpFECMaxSpan)        | [202]            | n/a | c32 | [202]            | n/a | c32 |
| 74 | T38 FAX Modem Type (a=T38ModemType)                         | [202]            | n/a | c32 | [202]            | n/a | c32 |
| 75 | T38 FAX Vendor Info (a=T38VendorInfo)                       | [202]            | n/a | c32 | [202]            | n/a | c32 |
| 76 | reduced-size RTCP (a=rtcp-rsize)                            | [204]            | c33 | c33 | [204]            | c34 | c34 |
| 77 | RTP control protocol extended report parameters (a=rtcp-xr) | [205]            | c35 | c35 | [205]            | c36 | c36 |
| 78 | maximum receive SDU size (a=3gpp_MaxRecvSDUSize)            | [9B]             | c37 | c37 | [9B]             | c38 | c38 |
| 79 | content (a=content)   | [206]            | c39 | c39 | [206]            | c39 | c39 |
| 85 | CS correlation (a=cs-correlation)                           | [155]<br>5.2.3.1 | c49 | c49 | [155]<br>5.2.3.1 | c49 | c49 |



|      |   |
|------|---|
| c1:  | IF A.317/22 AND A.318/20 THEN o ELSE n/a - - integration of resource management and SIP, media level attribute name "a=".   |
| c2:  | IF A.317/22 AND A.318/20 THEN m ELSE n/a - - integration of resource management and SIP, media level attribute name "a=".   |
| c3:  | IF A.317/23 AND A.318/20 THEN o ELSE n/a - - grouping of media lines, media level attribute name "a=".  |
| c4:  | IF A.317/23 AND A.318/20 THEN m ELSE n/a - - grouping of media lines, media level attribute name "a=".  |
| c5:  | IF A.317/23 AND A.318/14 THEN o ELSE n/a - - grouping of media lines, session level attribute name "a=".  |
| c6:  | IF A.317/23 AND A.318/14 THEN m ELSE n/a - - grouping of media lines, session level attribute name "a=".  |
| c7:  | IF A.317/26 AND A.318/20 THEN m ELSE n/a - - TCP-based media transport in the session description protocol, media level attribute name "a=".  |
| c8:  | IF A.318/14 THEN o ELSE x - - session level attribute name "a=".  |
| c9:  | IF A.318/14 THEN m ELSE n/a - - session level attribute name "a=".  |
| c10: | IF A.318/20 THEN o ELSE x - - media level attribute name "a=".  |
| c11: | IF A.318/20 THEN m ELSE n/a - - media level attribute name "a=".  |
| c12: | IF A.317/27 AND A.318/20 THEN o ELSE n/a - - candidate IP addresses, media level attribute name "a=".   |
| c13: | IF A.317/27 AND A.318/20 THEN m ELSE n/a - - candidate IP addresses, media level attribute name "a=".   |
| c14: | IF A.317/28 AND A.318/20 THEN m ELSE n/a - - session description protocol format for binary floor control protocol streams, media level attribute name "a=".  |
| c15: | IF (A.317/29 AND A.318/20) THEN m ELSE n/a - - extended RTP profile for real-time transport control protocol (RTCP)-based feedback (RTP/AVPF), media level attribute name "a=".   |
| c16: | IF A.317/30 AND A.318/20 THEN m ELSE n/a - - SDP capability negotiation, media level attribute name "a=".   |
| c17: | IF A.317/32 AND A.318/20 THEN o ELSE n/a - - miscellaneous capabilities negotiation in the Session Description Protocol (SDP), media level attribute name "a=".   |
| c18: | IF A.317/32 AND A.318/20 THEN m ELSE n/a - - miscellaneous capabilities negotiation in the Session Description Protocol (SDP), media level attribute name "a=".   |
| c19: | IF A.317/33 AND (A.318/14 OR A.318/20) THEN o ELSE n/a - - bandwidth modifier packet rate parameter, media or session level attribute name "a=".  |
| c20: | IF A.317/34 AND A.317/36 AND 318/20 THEN m ELSE n/a - - Secure Real-time Transport Protocol, media plane security using SDES, media level attribute name "a=".  |
| c21: | IF A.317/34 AND A.317/35 AND 318/20 THEN m ELSE n/a - - Secure Real-time Transport Protocol, media plane security using KMS, media level attribute name "a=".   |
| c22: | IF A.317/37 AND A.318/20 THEN m ELSE n/a - - end to access edge media security, media level attribute name "a=".  |
| c23: | IF A.317/38 THEN m ELSE n/a - - SDP media capabilities negotiation.   |
| c24: | IF A.317/38 AND A.318/14 THEN m ELSE n/a - - SDP media capabilities negotiation, session level attribute name "a=".   |
| c25: | IF A.317/40 AND A.318/20 THEN m ELSE n/a - - message session relay protocol, media level attribute name "a=".   |
| c26: | IF A.317/41 AND A.318/20 THEN o ELSE n/a - - a SDP offer/answer mechanism to enable file transfer, media level attribute name "a=".   |
| c27: | IF A.317/41 AND A.318/20 AND (A.3A/31 OR A.3A/33) THEN m ELSE IF A.317/41 AND A.318/20 AND NOT (A.3A/31 OR A.3A/33) THEN o ELSE n/a - - a SDP offer/answer mechanism to enable file transfer, media level attribute name "a=", messaging application server, messaging participant. |
| c28: | IF A.317/41 AND A.318/20 THEN m ELSE n/a - - a SDP offer/answer mechanism to enable file transfer, media level attribute name "a=".   |
| c29: | IF A.317/42 AND A.318/20 THEN o ELSE n/a - - optimal media routeing, media level attribute name "a=".   |
| c30: | IF A.317/43 THEN m ELSE n/a - - ECN for RTP over UDP, media level attribute name "a=".  |
| c31: | IF A.317/44 AND A.318/20 THEN m ELSE n/a - - T.38 FAX, media level attribute name "a=".   |
| c32: | IF A.317/44 AND A.318/20 THEN o ELSE n/a - - T.38 FAX, media level attribute name "a=".   |
| c33: | IF A.317/45 AND A.318/20 THEN o ELSE n/a - - support for reduced-size RTCP, media level attribute name "a=".  |
| c34: | IF A.317/45 AND A.318/20 THEN m ELSE n/a - - support for reduced-size RTCP, media level attribute name "a=".  |
| c35: | IF A.317/46 AND A.318/20 AND A.318/14 THEN o ELSE n/a - - RTCP extended reports, media level attribute name "a=", session level attribute name "a=".  |
| c36: | IF A.317/46 AND A.318/20 AND A.318/14 THEN m ELSE n/a - - RTCP extended reports, media level attribute name "a=", session level attribute name "a=".  |
| c37: | IF A.317/47 AND A.318/20 AND A.318/14 THEN o ELSE n/a - - maximum receive SDU size, media level attribute name "a=", session level attribute name "a=".   |
| c38: | IF A.317/47 AND A.318/20 AND A.318/14 THEN m ELSE n/a - - maximum receive SDU size, media level attribute name "a=", session level attribute name "a=".   |
| c39: | IF A.317/48 AND A.318/20 THEN m ELSE n/a - - the SDP content attribute, media level attribute name "a=".  |
| c44: | IF A.317/38 AND A.318/20 THEN m ELSE n/a - - SDP media capabilities negotiation, media level attribute name "a=".   |

|         |  |
|---------|--|
| c49:    | IF A.317/31 AND A.318/20 THEN m ELSE n/a - - Session Description Protocol (SDP) extension for setting up audio media streams over circuit-switched bearers in the Public Switched Telephone Network (PSTN) and SIP, media level attribute name "a=". |
| NOTE 1: | Further specification of the usage of this attribute is defined by specifications relating to individual codecs.   |

### A.3.2.3 Void

**Table A.320: Void**

**Table A.321: Void**

**Table A.322: Void**

**Table A.323: Void**

**Table A.324: Void**

**Table A.325: Void**

**Table A.326: Void**

**Table A.327: Void**

### A.3.2.4 Void

**Table A.327A: Void**

## A.3.3 Proxy role

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for proxy implementations.

Prerequisite: A.2/2 -- proxy role

## A.3.3.1 Major capabilities

Table A.328: Major capabilities

| Item | Does the implementation support  | Reference | RFC status | Profile status |
|------|--|-----------|------------|----------------|
|      | <b>Capabilities within main protocol</b>   |           |            |                |
| 0A   | application of session policy?   | 6.2, 6.3  | x          | c2             |
|      | <b>Extensions</b>  |           |            |                |
| 1    | integration of resource management and SIP?  | [30] [64] | o          | n/a            |
| 2    | grouping of media lines?   | [53]      | c3         | x              |
| 3    | mapping of media streams to resource reservation flows?  | [54]      | o          | x              |
| 4    | SDP bandwidth modifiers for RTCP bandwidth?  | [56]      | o          | c1             |
| 5    | TCP-based media transport in the session description protocol?   | [83]      | o          | c11            |
| 6    | interactive connectivity establishment?  | [99]      | o          | c4             |
| 7    | session description protocol format for binary floor control protocol streams?   | [108]     | o          | o              |
| 8    | extended RTP profile for real-time transport control protocol (RTCP)-based feedback (RTP/AVPF)?  | [135]     | o          | c5             |
| 9    | SDP capability negotiation?  | [137]     | o          | c9             |
| 10   | Session Description Protocol (SDP) extension for setting up audio media streams over circuit-switched bearers in the Public Switched Telephone Network (PSTN)?   | [155]     | o          | c6             |
| 11   | miscellaneous capabilities negotiation in the Session Description Protocol (SDP)?  | [156]     | o          | c6             |
| 14   | Secure Real-time Transport Protocol (SRTP)?  | [169]     | o          | o              |
| 15   | MIKEY-TICKET?  | [170]     | o          | o              |
| 16   | SDES?  | [168]     | o          | o              |
| 17   | end to access edge media security?   | 7.5.2     | n/a        | n/a            |
| 18   | SDP media capabilities negotiation?  | [172]     | o          | c8             |
| 19   | Transcoding Services Invocation in the Session Initiation Protocol (SIP) Using Third Party Call Control (3pcc)?  | [166]     | m          | i              |
| 20   | Message Session Relay Protocol?  | [178]     | o          | o              |
| 21   | a SDP offer/answer mechanism to enable file transfer?  | [185]     | o          | o              |
| 22   | optimal media routing?   | [11D]     | n/a        | o              |
| 23   | ECN for RTP over UDP?  | [188]     | o          | c10            |
| 24   | T.38 FAX?  | [202]     | n/a        | o              |
| 25   | support for reduced-size RTCP?   | [204]     | o          | o              |
| 26   | RTCP extended reports?   | [205]     | o          | o              |
| 27   | maximum receive SDU size?  | [9B]      | o          | o              |
| 28   | the SDP content attribute  | [206]     | o          | o              |
| c1:  | IF A.3/2 OR A.3A/88 THEN m ELSE n/a - - P-CSCF, ATCF (proxy).  |           |            |                |
| c2:  | IF A.3/2 OR A.3/4 THEN o ELSE x - P-CSCF, S-CSCF.  |           |            |                |
| c3:  | IF A.328/3 THEN m ELSE o - - mapping of media streams to resource reservation flows.   |           |            |                |
| c4:  | IF A.3/2 OR A.3/4 THEN m ELSE n/a - - P-CSCF, S-CSCF.  |           |            |                |
| c5:  | IF (A.3A/50A AND A.3/7C) OR A.3/2 OR A.3/4 OR A.3A/88 THEN m ELSE n/a - - multimedia telephony service application server as AS acting as a SIP proxy, P-CSCF, S-CSCF, ATCF (proxy).   |           |            |                |
| c6:  | IF (A.3A/83 AND A.3/7C) OR A.3/4 THEN m ELSE IF A.3A/88 THEN i ELSE n/a - - SCC application server, AS acting as a SIP proxy, S-CSCF, ATCF (proxy).  |           |            |                |
| c7:  | IF A.328/18 THEN m ELSE o - - SDP media capabilities negotiation.  |           |            |                |
| c8:  | IF A.3/2 OR A.3/4 THEN m ELSE IF A.3A/88 THEN i ELSE o - - P-CSCF, S-CSCF, ATCF (proxy).   |           |            |                |
| c9:  | IF (A.3A/50A AND A.3/7C) OR A.3/2 OR A.3/4 OR A.328/18 OR A.3A/88 THEN m ELSE n/a - - multimedia telephony service application server as AS acting as a SIP proxy, P-CSCF, S-CSCF, SDP media capabilities negotiation, ATCF (proxy). |           |            |                |
| c10: | IF A.3A/88 THEN o ELSE i - - ATCF (proxy).   |           |            |                |
| c11: | IF A.3/2 OR A.3/4 OR A.3A/88 THEN m ELSE n/a - - P-CSCF, S-CSCF, ATCF (proxy).   |           |            |                |

## A.3.3.2 SDP types

Table A.329: SDP types

| Item  | Type   | Sending   |            |                | Receiving |            |                |
|---|--|-----------|------------|----------------|-----------|------------|----------------|
|   |  | Ref.      | RFC status | Profile status | Ref.      | RFC status | Profile status |
| <b>Session level description</b>                        |  |           |            |                |           |            |                |
| 1   | v= (protocol version)  | [39] 5.1  | m          | m              | [39] 5.1  | m          | m              |
| 2   | o= (owner/creator and session identifier).                   | [39] 5.2  | m          | m              | [39] 5.2  | i          | i              |
| 3   | s= (session name)  | [39] 5.3  | m          | m              | [39] 5.3  | i          | i              |
| 4   | i= (session information)                                     | [39] 5.4  | m          | m              | [39] 5.4  | i          | i              |
| 5   | u= (URI of description)                                      | [39] 5.5  | m          | m              | [39] 5.5  | i          | i              |
| 6   | e= (email address)   | [39] 5.6  | m          | m              | [39] 5.6  | i          | i              |
| 7   | p= (phone number)  | [39] 5.6  | m          | m              | [39] 5.6  | i          | i              |
| 8   | c= (connection information)                                  | [39] 5.7  | m          | m              | [39] 5.7  | i          | i              |
| 9   | b= (bandwidth information)                                   | [39] 5.8  | m          | m              | [39] 5.8  | i          | i              |
| <b>Time description (one or more per description)</b>   |  |           |            |                |           |            |                |
| 10  | t= (time the session is active)                              | [39] 5.9  | m          | m              | [39] 5.9  | i          | i              |
| 11  | r= (zero or more repeat times)                               | [39] 5.10 | m          | m              | [39] 5.10 | i          | i              |
| <b>Session level description (continued)</b>            |  |           |            |                |           |            |                |
| 12  | z= (time zone adjustments)                                   | [39] 5.11 | m          | m              | [39] 5.11 | i          | i              |
| 13  | k= (encryption key)  | [39] 5.12 | m          | m              | [39] 5.12 | i          | i              |
| 14  | a= (zero or more session attribute lines)                    | [39] 5.13 | m          | m              | [39] 5.13 | i          | i              |
| <b>Media description (zero or more per description)</b> |  |           |            |                |           |            |                |
| 15  | m= (media name and transport address)                        | [39] 5.14 | m          | m              | [39] 5.14 | m          | m              |
| 16  | i= (media title)   | [39] 5.4  | m          | m              | [39] 5.4  | i          | i              |
| 17  | c= (connection information)                                  | [39] 5.7  | m          | m              | [39] 5.7  | i          | i              |
| 18  | b= (bandwidth information)                                   | [39] 5.8  | m          | m              | [39] 5.8  | i          | c1             |
| 19  | k= (encryption key)  | [39] 5.12 | m          | m              | [39] 5.12 | i          | i              |
| 20  | a= (zero or more media attribute lines)                      | [39] 5.13 | m          | m              | [39] 5.13 | i          | c1             |
| c1:   | IF A.328/0A THEN m ELSE i - - application of session policy. |           |            |                |           |            |                |

Prerequisite A.329/14 OR A.329/20 - - a= (zero or more session/media attribute lines)

**Table A.330: zero or more session / media attribute lines (a=)**

| Item | Field  | Sending                    |            |                | Receiving                  |            |                |
|------|--|----------------------------|------------|----------------|----------------------------|------------|----------------|
|      |  | Ref.                       | RFC status | Profile status | Ref.                       | RFC status | Profile status |
| 1    | category (a=cat)                                     | [39] 6                     | m          | m              | [39] 6                     | i          | i              |
| 2    | keywords (a=keywds)                                  | [39] 6                     | m          | m              | [39] 6                     | i          | i              |
| 3    | name and version of tool (a=tool)                    | [39] 6                     | m          | m              | [39] 6                     | i          | i              |
| 4    | packet time (a=ptime)                                | [39] 6                     | m          | m              | [39] 6                     | i          | c9             |
| 5    | maximum packet time (a=maxptime)                     | [39] 6<br>(NOTE 1)         | m          | m              | [39] 6<br>(NOTE 1)         | i          | c9             |
| 6    | receive-only mode (a=recvonly)                       | [39] 6                     | m          | m              | [39] 6                     | i          | c9             |
| 7    | send and receive mode (a=sendrecv)                   | [39] 6                     | m          | m              | [39] 6                     | i          | c9             |
| 8    | send-only mode (a=sendonly)                          | [39] 6                     | m          | m              | [39] 6                     | i          | c9             |
| 8A   | Inactive mode (a=inactive)                           | [39] 6                     | m          | m              | [39] 6                     | i          | c9             |
| 9    | whiteboard orientation (a=orient)                    | [39] 6                     | m          | m              | [39] 6                     | i          | c9             |
| 10   | conference type (a=type)                             | [39] 6                     | m          | m              | [39] 6                     | i          | i              |
| 11   | character set (a=charset)                            | [39] 6                     | m          | m              | [39] 6                     | i          | i              |
| 12   | language tag (a=sdplang)                             | [39] 6                     | m          | m              | [39] 6                     | i          | c9             |
| 13   | language tag (a=lang)                                | [39] 6                     | m          | m              | [39] 6                     | i          | c9             |
| 14   | frame rate (a=framerate)                             | [39] 6                     | m          | m              | [39] 6                     | i          | c9             |
| 15   | quality (a=quality)                                  | [39] 6                     | m          | m              | [39] 6                     | i          | c9             |
| 16   | format specific parameters (a=fmtp)                  | [39] 6                     | m          | m              | [39] 6                     | i          | c9             |
| 17   | rtpmap attribute (a=rtpmap)                          | [39] 6                     | m          | m              | [39] 6                     | i          | c9             |
| 18   | current-status attribute (a=curr)                    | [30] 5                     | m          | m              | [30] 5                     | c2         | c2             |
| 19   | desired-status attribute (a=des)                     | [30] 5                     | m          | m              | [30] 5                     | c2         | c2             |
| 20   | confirm-status attribute (a=conf)                    | [30] 5                     | m          | m              | [30] 5                     | c2         | c2             |
| 21   | media stream identification attribute (a=mid)        | [53] 3                     | c5         | x              | [53] 3                     | c6         | x              |
| 22   | group attribute (a=group)                            | [53] 4                     | c5         | x              | [53] 4                     | c6         | x              |
| 23   | setup attribute (a=setup)                            | [83] 4                     | c7         | c7             | [83] 4                     | c8         | c8             |
| 24   | connection attribute (a=connection)                  | [83] 5                     | c7         | c7             | [83] 5                     | c8         | c8             |
| 25   | candidate IP addresses (a=candidate)                 | [99]                       | c9         | c9             | [99]                       | c10        | c10            |
| 26   | floor control server determination (a=floorctrl)     | [108] 4                    | c11        | c11            | [108] 4                    | c12        | c13            |
| 27   | conference id (a=confid)                             | [108] 5                    | c11        | c11            | [108] 5                    | c12        | c13            |
| 28   | user id (a=userid)                                   | [108] 5                    | c11        | c11            | [108] 5                    | c12        | c13            |
| 29   | association between streams and floors (a=floorid)   | [108] 6                    | c11        | c11            | [108] 6                    | c12        | c13            |
| 30   | RTCP feedback capability attribute (a=rtcp-fb)       | [135] 4.2                  | c14        | c14            | [135] 4.2                  | c15        | c15            |
| 31   | extension of the rtcp-fb attribute (a=rtcp-fb)       | [136] 7.1<br>[188] 6.2     | c14        | c14            | [136] 7.1                  | c15        | c15            |
| 32   | supported capability negotiation extensions (a=csup) | [137] 3.3.1                | c16        | c16            | [137] 3.3.1                | c17        | c17            |
| 33   | required capability negotiation extensions (a=creq)  | [137] 3.3.2                | c16        | c16            | [137] 3.3.2                | c17        | c17            |
| 34   | attribute capability (a=acap)                        | [137] 3.4.1                | c16        | c16            | [137] 3.4.1                | c17        | c17            |
| 35   | transport protocol capability (a=tcap)               | [137] 3.4.2                | c16        | c16            | [137] 3.4.2                | c17        | c17            |
| 36   | potential configuration (a=pcfg)                     | [137] 3.5.1<br>[172] 3.3.6 | c16        | c16            | [137] 3.5.1<br>[172] 3.3.6 | c17        | c17            |
| 37   | actual configuration (a=acfg)                        | [137] 3.5.2                | c16        | c16            | [137] 3.5.2                | c17        | c17            |

|     |   |                |     |     |                |     |     |
|-----|---|----------------|-----|-----|----------------|-----|-----|
| 38  | connection data capability (a=ccap)                           | [156] 3.1      | c18 | c18 | [156] 3.1      | c19 | c19 |
| 40  | crypto attribute (a=crypto)                                   | [168]          | c20 | c20 | [167]          | c20 | c20 |
| 41  | key management attribute (a=key-mgmt)                         | [167]          | c21 | c21 | [168]          | c22 | c22 |
| 42  | 3GPP_e2ae-security-indicator (a=3ge2ae)                       | 7.5.2          | c23 | c23 | 7.5.2          | c23 | c23 |
| 43  | media capability (a=rmcap)                                    | [172]<br>3.3.1 | c24 | c24 | [172]<br>3.3.1 | c26 | c26 |
| 43A | media capability (a=omcap)                                    | [172]<br>3.3.1 | c24 | c24 | [172]<br>3.3.1 | c26 | c26 |
| 44  | media format capability (a=mfcap)                             | [172]<br>3.3.2 | c24 | c24 | [172]<br>3.3.2 | c26 | c26 |
| 45  | media-specific capability (a=mscap)                           | [172]<br>3.3.3 | c24 | c24 | [172]<br>3.3.3 | c26 | c26 |
| 46  | latent configuration (a=lcfg)                                 | [172]<br>3.3.5 | c48 | c48 | [172]<br>3.3.5 | c49 | c49 |
| 47  | session capability (a=sescap)                                 | [172]<br>3.3.8 | c25 | c25 | [172]<br>3.3.8 | c27 | c27 |
| 48  | msrp path (a=path)  | [178]          | c28 | c28 | [178]          | c29 | c29 |
| 49  | file selector (a=file-selector)                               | [185] 6        | c30 | c30 | [185] 6        | c31 | c31 |
| 50  | file transfer identifier (a= file-transfer-id)                | [185] 6        | c30 | c30 | [185] 6        | c31 | c31 |
| 51  | file disposition (a=file-disposition)                         | [185] 6        | c30 | c30 | [185] 6        | c31 | c31 |
| 52  | file date (a=file-date)                                       | [185] 6        | c30 | c30 | [185] 6        | c31 | c31 |
| 53  | file icon (a=file-icon)                                       | [185] 6        | c30 | c30 | [185] 6        | c31 | c31 |
| 54  | file range (a=file-range)                                     | [185] 6        | c30 | c30 | [185] 6        | c31 | c31 |
| 55  | optimal media routeing visited realm (a=visited-realm)        | 7.5.3          | c32 | c32 | 7.5.3          | c33 | c33 |
| 56  | optimal media routeing secondary realm (a=secondary-realm)    | 7.5.3          | c32 | c32 | 7.5.3          | c33 | c33 |
| 57  | optimal media routeing media level checksum (a=omr-m-cksum)   | 7.5.3          | c32 | c32 | 7.5.3          | c33 | c33 |
| 58  | optimal media routeing session level checksum (a=omr-s-cksum) | 7.5.3          | c32 | c32 | 7.5.3          | c33 | c33 |
| 59  | optimal media routeing codecs (a=omr-codecs)                  | 7.5.3          | c32 | c32 | 7.5.3          | c33 | c33 |
| 60  | optimal media routeing media attributes (a=omr-m-att)         | 7.5.3          | c32 | c32 | 7.5.3          | c33 | c33 |
| 61  | optimal media routeing session attributes (a=omr-s-att)       | 7.5.3          | c32 | c32 | 7.5.3          | c33 | c33 |
| 62  | optimal media routeing media bandwidth (a=omr-m-bw)           | 7.5.3          | c32 | c32 | 7.5.3          | c33 | c33 |
| 63  | optimal media routeing session bandwidth (a=omr-s-bw)         | 7.5.3          | c32 | c32 | 7.5.3          | c33 | c33 |
| 64  | ecn-attribute (a=ecn-capable-rtt)                             | [188]          | c34 | c34 | [188]          | c34 | c34 |
| 65  | T38 FAX Protocol version (a=T38FaxVersion)                    | [202]          | n/a | c35 | [202]          | n/a | c36 |
| 66  | T38 FAX Maximum Bit Rate (a=T38MaxBitRate)                    | [202]          | n/a | c35 | [202]          | n/a | c36 |
| 67  | T38 FAX Rate Management (a=T38FaxRateManagement)              | [202]          | n/a | c35 | [202]          | n/a | c36 |
| 68  | T38 FAX Maximum Buffer Size (a=T38FaxMaxBuffer)               | [202]          | n/a | c35 | [202]          | n/a | c36 |
| 69  | T38 FAX Maximum Datagram Size (a=T38FaxMaxDatagram)           | [202]          | n/a | c35 | [202]          | n/a | c36 |
| 70  | T38 FAX maximum IFP frame size (a=T38FaxMaxIFP)               | [202]          | n/a | c35 | [202]          | n/a | c36 |

|    |   |                  |     |     |                  |     |     |
|----|---|------------------|-----|-----|------------------|-----|-----|
| 71 | T38 FAX UDP Error Correction Scheme (a=T38FaxUdpEC)         | [202]            | n/a | c35 | [202]            | n/a | c36 |
| 72 | T38 FAX UDP Error Correction Depth (a=T38FaxUdpECDepth)     | [202]            | n/a | c35 | [202]            | n/a | c36 |
| 73 | T38 FAX UDP FEC Maximum Span (a=T38FaxUdpFECMaxSpan)        | [202]            | n/a | c35 | [202]            | n/a | c36 |
| 74 | T38 FAX Modem Type (a=T38ModemType)                         | [202]            | n/a | c35 | [202]            | n/a | c36 |
| 75 | T38 FAX Vendor Info (a=T38VendorInfo)                       | [202]            | n/a | c35 | [202]            | n/a | c36 |
| 76 | reduced-size RTCP (a=rtcp-rsize)                            | [204]            | c37 | c37 | [204]            | c38 | c38 |
| 77 | RTP control protocol extended report parameters (a=rtcp-xr) | [205]            | c39 | c39 | [205]            | c40 | c40 |
| 78 | maximum receive SDU size (a=3gpp_MaxRecvSDUSize)            | [9B]             | c41 | c41 | [9B]             | c42 | c42 |
| 79 | content (a=content)   | [206]            | c43 | c43 | [206]            | c43 | c43 |
| 85 | CS correlation (a=cs-correlation)                           | [155]<br>5.2.3.1 | c57 | c57 | [155]<br>5.2.3.1 | c57 | c57 |



|      |  |
|------|--|
| c2:  | IF A.328/1 THEN m ELSE i - - integration of resource management and SIP.   |
| c5:  | IF A.328/2 THEN m ELSE n/a - - grouping of media lines.  |
| c6:  | IF A.328/3 THEN m ELSE IF A.328/2 THEN i ELSE n/a - - mapping of media streams to resource reservation flows, grouping of media lines.   |
| c7:  | IF A.328/5 THEN m ELSE n/a.  |
| c8:  | IF A.328/5 THEN i ELSE n/a.  |
| c9:  | IF A.329/20 AND A.328/0A THEN m ELSE i - - media level attribute name "a=" and application of session policy.  |
| c9:  | IF A.328/6 THEN m ELSE n/a - - interactive connectivity establishment.   |
| c10: | IF A.328/1 AND A.328/6 THEN m ELSE IF A.328/6 THEN i ELSE n/a - - integration of resource management and SIP, interactive connectivity establishment.  |
| c11: | IF A.328/7 THEN m ELSE n/a - - session description protocol format for binary floor control protocol streams.  |
| c12: | IF A.328/7 THEN i ELSE n/a - - session description protocol format for binary floor control protocol streams.  |
| c13: | IF A.328/7 AND A.328/0A AND A.329/20 THEN m ELSE IF A.328/7 AND A.329/20 THEN i ELSE n/a - - session description protocol format for binary floor control protocol streams, media level attribute name "a=" and application of session policy. |
| c14: | IF (A.328/8 AND A.329/20) THEN m ELSE n/a - - extended RTP profile for real-time transport control protocol (RTCP)-based feedback (RTP/AVPF), media level attribute name "a=".   |
| c15: | IF (A.328/8 AND A.329/20) THEN i ELSE n/a - - extended RTP profile for real-time transport control protocol (RTCP)-based feedback (RTP/AVPF), media level attribute name "a=".   |
| c16: | IF A.328/9 AND A.329/20 THEN m ELSE n/a - - SDP capability negotiation, media level attribute name "a=".   |
| c17: | IF A.328/9 AND A.329/20 THEN i ELSE n/a - - SDP capability negotiation, media level attribute name "a=".   |
| c18: | IF A.328/11 AND A.329/20 THEN o ELSE n/a - - miscellaneous capabilities negotiation in the Session Description Protocol (SDP), media level attribute name "a=".  |
| c19: | IF A.328/11 AND A.329/20 THEN m ELSE n/a - - miscellaneous capabilities negotiation in the Session Description Protocol (SDP), media level attribute name "a=".  |
| c20: | IF A.328/14 AND A.328/16 AND A.329/20 THEN m ELSE n/a - - Secure Real-time Transport Protocol, media plane security using SDES, media level attribute name "a=".   |
| c21: | IF A.328/14 AND A.328/15 AND A.329/20 THEN m ELSE n/a - - Secure Real-time Transport Protocol, media plane security using KMS, media level attribute name "a=".  |
| c22: | IF A.328/14 AND A.328/15 AND A.329/20 THEN i ELSE n/a - - Secure Real-time Transport Protocol, media plane security using KMS, media level attribute name "a=".  |
| c23: | IF A.328/17 AND A.329/20 THEN m ELSE n/a - - end to access edge media security, media level attribute name "a=".   |
| c24: | IF A.328/18 THEN m ELSE n/a - - SDP media capabilities negotiation.  |
| c25: | IF A.328/18 AND A.329/14 THEN m ELSE n/a - - SDP media capabilities negotiation, session level attribute name "a=".  |
| c26: | IF A.328/18 AND A.328/0A THEN m ELSE IF A.328/18 THEN i ELSE n/a - - SDP media capabilities negotiation, application of session policy.  |
| c27: | IF A.328/18 AND A.329/14 AND A.328/0A THEN m ELSE IF A.328/18 AND A.329/14 THEN i ELSE n/a - - SDP media capabilities negotiation, session level attribute name "a=", application of session policy.   |
| c28: | IF A.328/20 AND A.329/20 THEN m ELSE n/a - - message session relay protocol, media level attribute name "a=".  |
| c29: | IF A.328/20 AND A.329/20 THEN i ELSE n/a - - message session relay protocol, media level attribute name "a=".  |
| c30: | IF A.328/21 AND A.329/20 THEN m ELSE n/a - - a SDP offer/answer mechanism to enable file transfer, media level attribute name "a=".  |
| c31: | IF A.328/21 AND A.329/20 THEN i ELSE n/a - - a SDP offer/answer mechanism to enable file transfer, media level attribute name "a=".  |
| c32: | IF A.328/22 AND A.329/20 THEN m ELSE n/a - - optimal media routing, media level attribute name "a=".   |
| c33: | IF A.328/22 AND A.329/20 THEN i ELSE n/a - - optimal media routing, media level attribute name "a=".   |
| c34: | IF A.328/23 THEN m ELSE i - - ECN for RTP over UDP, media level attribute name "a=".   |
| c35: | IF A.328/24 AND A.329/20 THEN m ELSE n/a - - T.38 FAX, media level attribute name "a=".  |
| c36: | IF A.328/24 AND A.329/20 THEN i ELSE n/a - - T.38 FAX, media level attribute name "a=".  |
| c37: | IF A.328/25 AND A.329/20 THEN m ELSE n/a - - support for reduced-size RTCP, media level attribute name "a=".   |
| c38: | IF A.328/25 AND A.329/20 THEN i ELSE n/a - - support for reduced-size RTCP, media level attribute name "a=".   |
| c39: | IF A.328/26 AND A.329/20 AND A.329/14 THEN m ELSE n/a -- RTCP extended reports, media level attribute name "a=", session level attribute name "a=".  |
| c40: | IF A.328/26 AND A.329/20 AND A.329/14 THEN i ELSE n/a -- RTCP extended reports, media level attribute name "a=", session level attribute name "a=".  |
| c41: | IF A.328/27 AND A.329/20 AND A.329/14 THEN m ELSE n/a -- maximum receive SDU size, media level attribute name "a=", session level attribute name "a=".   |
| c42: | IF A.328/27 AND A.329/20 AND A.329/14 THEN i ELSE n/a -- maximum receive SDU size, media level attribute name "a=", session level attribute name "a=".   |

|  |  |
|--|--|
| c43:   | IF A.328/28 AND A.329/20 THEN m ELSE n/a - - the SDP content attribute, media level attribute name "a=".   |
| c48:   | IF A.328/18 AND A.329/20 THEN m ELSE n/a - - SDP media capabilities negotiation, media level attribute name "a=".  |
| c49:   | IF A.328/18 AND A.329/20 AND A.328/0A THEN m ELSE IF A.328/18 AND A.329/20 THEN i ELSE n/a - - SDP media capabilities negotiation, media level attribute name "a=", application of session policy.   |
| c57:   | IF A.318/10 AND A.329/20 THEN m ELSE n/a - - Session Description Protocol (SDP) extension for setting up audio media streams over circuit-switched bearers in the Public Switched Telephone Network (PSTN) and SIP, media level attribute name "a=". |
| NOTE 1: Further specification of the usage of this attribute is defined by specifications relating to individual codecs. |  |

### A.3.3.3 Void

**Table A.331: Void**

**Table A.332: Void**

**Table A.333: Void**

**Table A.334: Void**

**Table A.335: Void**

**Table A.336: Void**

**Table A.337: Void**

**Table A.338: Void**

### A.3.3.4 Void

**Table A.339: Void**

---

## A.4 Profile definition for other message bodies as used in the present document

Void.

---

# Annex B (normative): IP-Connectivity Access Network specific concepts when using GPRS to access IM CN subsystem

## B.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is General Packet Radio Service (GPRS). The GPRS IP-CAN has a GPRS core network which can be supported by GERAN and UTRAN radio access networks. The present annex also defines procedures for invoking CS domain services.

---

## B.2 GPRS aspects when connected to the IM CN subsystem

### B.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by GPRS to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the UE on the use of these packet-mode services are specified in this clause. Requirements for the GGSN in support of this communication are specified in 3GPP TS 29.061 [11], 3GPP TS 29.207 [12] and 3GPP TS 29.212 [13B].

When using the GPRS, each IP-CAN bearer is provided by a PDP context.

### B.2.2 Procedures at the UE

#### B.2.2.1 PDP context activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

- a) if not attached for GPRS services yet, perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];
- b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

NOTE 1: During the PDP context activation procedure, the UE and network negotiate whether the UE or the GPRS IP-CAN is responsible for the resource reservation applicable to all PDP contexts within the activated PDP address/APN pair, as described in 3GPP TS 24.008 [8].

When the bearer establishment is controlled by the UE, the UE shall choose one of the following options when performing establishment of this PDP context:

I. A dedicated PDP context for SIP signalling:

The UE shall indicate to the GGSN that this is a PDP context intended to carry IM CN subsystem-related signalling only by setting the IM CN Subsystem Signalling Flag. The UE may also use this PDP context for DNS and DHCP signalling according to the static packet filters as described in 3GPP TS 29.061 [11]. The UE can also set the Signalling Indication attribute within the QoS information element;

II. A general-purpose PDP context:

The UE may decide to use a general-purpose PDP Context to carry IM CN subsystem-related signalling. The UE shall indicate to the GGSN that this is a general-purpose PDP context by not setting the IM CN

Subsystem Signalling Flag. The UE may carry both signalling and media on the general-purpose PDP context. The UE can also set the Signalling Indication attribute within the QoS information element.

NOTE 2: When the bearer establishment is controlled by the GPRS IP-CAN, the GGSN follows the procedures described in 3GPP TS 29.061 [11] in order to establish a dedicated PDP context for SIP signalling.

The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message. Upon successful signalling PDP context establishment the UE receives an indication from GGSN in the form of IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element. If the flag is not received, the UE shall consider the PDP context as a general-purpose PDP context.

The encoding of the IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

The UE can indicate a request for prioritised handling over the radio interface by setting the Signalling Indication attribute (see 3GPP TS 23.107 [4A]). The general QoS negotiation mechanism and the encoding of the Signalling Indication attribute within the QoS information element are described in 3GPP TS 24.008 [8].

NOTE 3: A general-purpose PDP Context can carry both IM CN subsystem signalling and media, in case the media does not need to be authorized by Policy and Charging control mechanisms as defined in 3GPP TS 29.212 [13B] and Service Based Local Policy mechanisms defined in 3GPP TS 29.207 [12] and the media stream is not mandated by the P-CSCF to be carried in a separate PDP Context.

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

- I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.
- II. Transfer P-CSCF address(es) within the PDP context activation procedure.

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

If the GGSN provides the UE with a list of P-CSCF IPv4 or IPv6 addresses in the ACTIVATE PDP CONTEXT ACCEPT message or ACTIVATE SECONDARY PDP CONTEXT ACCEPT message, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options information element as the P-CSCF address with the highest priority.

III. The UE selects a P-CSCF from the list (see 3GPP TS 31.103 [15B]) stored in the ISIM.

IV. The UE selects a P-CSCF from the list in IMS management object.

The UE shall use method IV to select a P-CSCF, if:

- a P-CSCF is to be discovered in the home network;
- the UE is roaming; and
- the IMS management object contains the P-CSCF list.

The UE shall use method III to select the P-CSCF, if:

- a P-CSCF is to be discovered in the home network;
- the UE is roaming;
- either the UE does not contain the IMS management object, or the UE contains the IMS management object, but the IMS management object does not contain the P-CSCF list; and

- the ISIM residing in the UICC supports the P-CSCF list.

The UE can freely select method I or II for P-CSCF discovery, if:

- the UE is in the home network; or
- the UE is roaming and the P-CSCF is to be discovered in the visited network.

In case method I is selected and several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3361 [35A] when using IPv4 or RFC 3319 [41] when using IPv6. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

NOTE 4: The UE decides whether the P-CSCF is to be discovered in the serving network or in the home network based on local configuration, e.g. whether the application on the UE is permitted to use local breakout.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

If the UE is configured to use Option II above and detects that all P-CSCFs known by the UE have been used when the UE selects a different P-CSCF as a result of:

- receiving 305 (Use Proxy) to the REGISTER request;
- receiving 504 (Server Time-out); or
- expiration of the timer F at the UE,

then the UE should:

- release IP-CAN bearer that is used only for the transport of SIP signalling and that are not used for other non-IMS applications, except emergency IP-CAN bearers;
- perform a new P-CSCF discovery procedure as described in subclause 9.2.1; and
- perform the procedures for initial registration as described in subclause 5.1.1.2.

NOTE 5: The UE may not be able to release the IP-CAN bearer if the IP-CAN bearer is in use by other applications.

When using IPv4, the UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

When using IPv6, the UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

The encoding of the request and response for IPv4 or IPv6 address(es) for DNS server(s) and list of P-CSCF address(es) within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

### B.2.2.1A Modification of a PDP context used for SIP signalling

The PDP context shall not be modified from a dedicated PDP context for SIP signalling to a general-purpose PDP context or vice versa. The IM CN Subsystem Signalling Flag shall not be set in the Protocol Configuration Options information element of the MODIFY PDP CONTEXT REQUEST message.

The UE shall not indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options information element of the MODIFY PDP CONTEXT REQUEST message. The UE shall ignore P-CSCF address(es) if received from the GGSN in the Protocol Configuration Options information element of the MODIFY PDP CONTEXT RESPONSE message.

### B.2.2.1B Re-establishment of the PDP context for SIP signalling

If the UE registered a public user identity with an IP address allocated for the APN of the PDP context used for SIP signalling, the PDP context used for SIP signalling is deactivated as result of signalling from the network (e.g. no longer available as a result of a successful GPRS routing area update procedure) and:

- i) if the signalling from the network results in requiring the UE to initiate activation of the PDP context used for SIP signalling; or
- ii) if the UE needs to continue having a public user identity registered with an IP address allocated for the APN;

and the UE is allowed to send:

- ACTIVATE PDP CONTEXT REQUEST message; or
- ACTIVATE SECONDARY PDP CONTEXT REQUEST message;

to activate the PDP context for SIP signalling, the UE shall:

- A) if the non-access stratum is performing the PDP context activation procedure for the APN triggered as result of the signalling from the network, wait until the PDP context activation procedure for the APN finishes; and
- B) perform the procedures in subclause B.2.2.1, bullets a), b) and c).

If:

- none of the bullets i) and ii) of this subclause evaluate to true;
- the UE is not allowed to send the ACTIVATE (SECONDARY) PDP CONTEXT REQUEST message;
- the procedures in bullet B) of this subclause were unable to ensure that the PDP context used for SIP signalling is available; or
- the procedures in bullet B) of this subclause were unable to acquire any P-CSCF address(es);

and if the PDP context used for SIP signalling was a dedicated PDP context for SIP signalling as described in subclause B.2.2.1, the UE shall deactivate all PDP contexts established as a result of SIP signalling according to the 3GPP TS 24.008 [8].

NOTE: 3GPP TS 24.008 [8] specifies conditions that prevent the UE from sending an ACTIVATE (SECONDARY) PDP CONTEXT REQUEST message.

If all PDP contexts for the APN were deactivated at the start of this subclause and the procedures in bullet B) of this subclause ensured that the PDP context used for SIP signalling is available and acquired the P-CSCF address(es), the UE shall perform a new initial registration according to subclause 5.1.1.2.

### B.2.2.1C P-CSCF restoration procedure

A UE supporting the P-CSCF restoration procedure performs one of the following procedures:

- A. if the UE used method II for P-CSCF discovery and if the UE receives the one or more P-CSCF address(es) in the Protocol Configuration Options information element of an MODIFY PDP CONTEXT REQUEST message and the one or more P-CSCF address(es) do not include the address of the currently used P-CSCF, then the UE shall acquire a different P-CSCF address from the one or more P-CSCF address(es) in the MODIFY PDP CONTEXT REQUEST message. If more than one P-CSCF address with the same container identifier (i.e. "P-CSCF IPv6 Address" or "P-CSCF IPv4 Address") are included, then the UE shall assume that the more than one P-CSCF addresses with the same container identifier are prioritised with the first P-CSCF address with the same container identifier within the Protocol Configuration Options information element as the P-CSCF address with the highest priority;
- B. if the UE uses RFC 6223 [143] as part of P-CSCF restoration procedures, and if the P-CSCF fails to respond to a keep-alive request, then the UE shall acquire a different P-CSCF address using one of the methods I, III and IV for P-CSCF discovery described in the subclause B.2.2.1.

When a different P-CSCF address is acquired the UE shall perform an initial registration as specified in subclause 5.1.

## B.2.2.2 Session management procedures

The existing procedures for session management as described in 3GPP TS 24.008 [8] shall apply while the UE is connected to the IM CN subsystem.

## B.2.2.3 Mobility management procedures

The existing procedures for mobility management as described in 3GPP TS 24.008 [8] shall apply while the UE is connected to the IM CN subsystem.

## B.2.2.4 Cell selection and lack of coverage

The existing mechanisms and criteria for cell selection as described in 3GPP TS 25.304 [9] and 3GPP TS 44.018 [20] shall apply while the UE is connected to the IM CN subsystem.

## B.2.2.5 PDP contexts for media

### B.2.2.5.1 General requirements

The UE can establish media streams that belong to different SIP sessions on the same PDP context.

During establishment of a session, the UE establishes data streams(s) for media related to the session. Such data stream(s) may result in activation of additional PDP context(s). Such additional PDP context(s) shall be established as secondary PDP contexts associated to the PDP context used for signalling. Such secondary PDP contexts for media can be established either by the UE or the GGSN.

If the bearer establishment is controlled by the UE, the UE starts reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available as specified in 3GPP TS 24.008 [8].

NOTE 1: If the bearer establishment is controlled by the GPRS IP CAN, the resource reservation requests are initiated by the GGSN after the P-CSCF has authorised the respective IP flows and provided the QoS requirements over the Rx interface to the PCRF, as described in 3GPP TS 29.214 [13D].

NOTE 2: When the UE has to allocate bandwidth for RTP and RTCP in a PDP context, the UE uses the rules as those outlined in 3GPP TS 29.213 [13C].

### B.2.2.5.1A Activation or modification of PDP contexts for media by the UE

If the UE is configured not to initiate resource allocation for media according to 3GPP TS 24.167 [8G] and both UE and network are allowed to establish the secondary PDP contents, then the UE shall refrain from establishing the secondary PDP context(s) for media and from modifying existing PDP contexts for media until the UE considers that the network did not initiate resource allocation for the media.

If the UE receives indication within the SDP according to RFC 3524 [54] that media stream(s) belong to group(s), the media stream(s) shall be set up on separate PDP contexts according to the indication of grouping of media streams. The UE may freely group media streams to PDP context(s) in case no indication of grouping of media streams is received from the P-CSCF.

If the capabilities of the originating UE prevents it from establishment of additional PDP contexts according to the media grouping attributes given by the P-CSCF in accordance with RFC 3524 [54], the UE will not establish such grouping of media streams. Instead, the originating UE shall negotiate media parameters for the session according to RFC 3264 [27B].

If the capabilities of the terminating UE prevents it from establishment of additional PDP contexts according to the media grouping attributes given by the P-CSCF in accordance with RFC 3524 [54], the UE will not establish such grouping of media streams. Instead, the terminating UE shall the UE shall handle such SDP offers in accordance with RFC 3388 [53].

The UE can receive a media authorization token in the P-Media-Authorization header field from the P-CSCF according to RFC 3313 [31]. If a media authorization token is received in the P-Media-Authorization header field when a SIP session is initiated, the UE shall:

- either use existing PDP context(s) where another media authorization token is already in use and no indication of grouping of media streams is required; or
- establish separate PDP context(s) for the media; or
- use an existing PDP context where media authorization token is not in use and no indication of grouping of media streams is required.

When a UE modifies a PDP context to indicate a new media authorization token:

- either as a result of establishment of an additional SIP session; or
- modification of media streams for an ongoing SIP session;

the UE shall include all media authorization tokens and all flow identifiers for all ongoing SIP sessions that use this particular PDP context.

If a media authorization token is received in subsequent messages for the same SIP session, the UE shall:

- use the existing PDP context(s) for media;
- modify the existing PDP context(s) for media; or
- establish additional PDP context(s) for media.

If either background or interactive QoS class is needed for the media, then the UE does not need to use the authorization token even if it receives one. In this case the UE may reuse an existing PDP context and it does not need to request PDP context modification unless it needs to modify the QoS.

If existing PDP context(s) where another media authorization token is already in use is re-used for the media, or separate PDP context(s) is established for the media, the UE shall proceed as follows:

- when a SIP session is terminated, the media authorization token is no longer valid and the UE shall not include it in future GPRS session management messages. The UE shall send a MODIFY PDP CONTEXT REQUEST message updating the binding information by deleting the media authorization token and the corresponding flow identifiers that are no longer valid. If a SIP session is terminated and no other SIP sessions are using the PDP context, the UE shall either update the binding information as described above or deactivate the PDP context;
- the UE shall transparently pass the media authorization token received from the P-CSCF in a response to an INVITE request at originating setup or in the INVITE request at terminating setup to the GGSN. The UE shall signal it by inserting it within the Traffic Flow Template information element in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message;
- to identify to the GGSN which flow(s) (identified by m-lines within the SDP) that are transferred within a particular PDP context, the UE shall set the flow identifier(s) within the Traffic Flow Template information element in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message. Detailed description of how the flow identifiers are constructed is provided in 3GPP TS 29.207 [12];
- if the UE receives several media authorization tokens from the P-CSCF within the same SIP request or response, the first instance of the media authorization token shall be sent to the GGSN, and subsequent instances are discarded by the UE; and
- the UE shall not include the IM CN Subsystem Signalling Flag when a PDP context for media is established or modified.

The encoding of the media authorization token and the flow identifiers within the Traffic Flow Template information element is described in 3GPP TS 24.008 [8].

#### B.2.2.5.1B Activation or modification of PDP contexts for media by the GGSN

If the UE receives an activation request from the GGSN for a PDP context which is associated with the PDP context used for signalling, the UE shall, based on the information contained in the Traffic Flow Template information element, correlate the media PDP context with a currently ongoing SIP session establishment or SIP session modification.



If the UE receives a modification request from the GGSN for a PDP context that is used for one or more media streams in an ongoing SIP session, the UE shall:

- 1) modify the related PDP context in accordance with the request received from the GGSN.

#### B.2.2.5.1C Deactivation of PDP context for media

When a data stream for media related to a session is released, if the PDP context transporting the data stream is no longer needed and if the PDP context has been activated by the UE, then the UE deactivates the PDP context.

NOTE: The PDP context can be needed e.g. for other data streams of a session or for other applications in the UE.

#### B.2.2.5.2 Special requirements applying to forked responses

NOTE 1: The procedures in this subclause only apply when the UE requests activation and modification of media bearers. In the case where the network activates and modifies the media bearers the network takes care of the handling of media bearers in the case of forking.

Since the UE does not know that forking has occurred until a second, provisional response arrives, the UE sets up the PDP context(s) as required by the initial response received. If a subsequent provisional response is received, different alternative actions may be performed depending on the requirements in the SDP answer:

- 1) the bearer requirements of the subsequent SDP can be accommodated by the existing PDP context(s). The UE performs no activation or modification of PDP contexts.
- 2) the subsequent SDP introduces different QoS requirements or additional IP flows. The UE modifies the existing PDP context(s), if necessary, according to subclause B.2.2.5.1A.
- 3) the subsequent SDP introduces one or more additional IP flows. The UE establishes additional PDP context(s) according to subclause B.2.2.5.1A.

NOTE 2: When several forked responses are received, the resources requested by the UE is are the "logical OR" of the resources indicated in the multiple responses to avoid allocation of unnecessary resources. The UE does not request more resources than proposed in the original INVITE request.

NOTE 3: When service-based local policy is applied, the UE receives the same authorization token for all forked requests/responses related to the same SIP session.

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall release all the unneeded radio/bearer resources. Therefore, upon the reception of the first final 200 (OK) response for the INVITE request (in addition to the procedures defined in RFC 3261 [26] subclause 13.2.2.4), the UE shall:

- 1) in case PDP context(s) were established or modified as a consequence of the INVITE request and forked provisional responses that are not related to the accepted 200 (OK) response, delete the PDP context(s) or modify the delete the PDP context(s) back to their original state.

#### B.2.2.5.3 Unsuccessful situations

One of the Go, Gq, Rx and Gx interface related error codes can be received by the UE in the ACTIVATE SECONDARY PDP CONTEXT REJECT message or the MODIFY PDP CONTEXT REJECT message. If the UE receives a Go, Gq, Rx and Gx interface related error code, the UE shall either handle the resource reservation failure as described in subclause 6.1.1 or retransmit the message up to three times. The Go, Gq, Rx and Gx interface related error codes are further specified in 3GPP TS 29.207 [12], 3GPP TS 29.209 [13A], 3GPP TS 29.214 [13D] and 3GPP TS 29.212 [13B].

#### B.2.2.6 Emergency service

Emergency bearers are defined for use in emergency calls in GPRS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these bearers for both signalling and media on emergency calls made using the IM CN subsystem.

Some jurisdictions allow emergency calls to be made when the UE does not contain an ISIM or USIM, or where the credentials are not accepted. Additionally where the UE is in state GMM-REGISTERED.LIMITED-SERVICE and GMM-REGISTERED.PLMN-SEARCH, a normal ATTACH has been attempted and it can also be assumed that a

registration in the IM CN subsystem will also fail. In such cases, the procedures for emergency calls without registration apply, as defined in subclause 5.1.6.8.2.

When activating a PDP context to perform emergency registration, the UE shall request a PDP context for emergency bearer services as defined in 3GPP TS 24.008 [8]. The procedures for PDP context activation and P-CSCF discovery, as described in subclause B.2.2.1 of this specification apply accordingly.

In order to find out whether the UE is attached to the home PLMN or to the visited PLMN, the UE shall compare the MCC and MNC values derived from its IMSI with the MCC and MNC of the PLMN the UE is attached to. If the MCC and MNC of the PLMN the UE is attached to do not match with the MCC and MNC derived from the IMSI, then for the purpose of emergency calls in the IM CN subsystem the UE shall consider to be attached to a VPLMN.

NOTE 1: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 [4C] will be considered as a visited network.

The type of emergency service for an emergency number is derived from the settings of the emergency service category value (bits 1 to 5 of the emergency service category value as specified in subclause 10.5.4.33 of 3GPP TS 24.008 [8]). Table B.2.2.6.1 below specifies mappings between a type of emergency service and an emergency service URN. The UE shall use the mapping to match an emergency service URN and a type of emergency service. If a dialled number is an emergency number but does not map to a type of emergency service the service URN shall be "urn:service:sos".

**Table B.2.2.6.1: Mapping between type of emergency service and emergency service URN**

| Type of emergency service | Emergency service URN     |
|---------------------------|---------------------------|
| Police                    | urn:service:sos.police    |
| Ambulance                 | urn:service:sos.ambulance |
| Fire Brigade              | urn:service:sos.fire      |
| Marine Guard              | urn:service:sos.marine    |
| Mountain Rescue           | urn:service:sos.mountain  |

NOTE 2: It is not possible for a UE to indicate more than one type of emergency service in an emergency service URN.

If the IP-CAN did not provide a local emergency number that matches the dialled number (see subclause 5.1.6.1) and multiple types of emergency service can be derived for a dialled number from the information configured on the USIM then:

- if the UE is in the HPLMN, the UE shall map any one of these types of emergency service to an emergency service URN as specified in table B.2.2.6.1; and
- if the UE is in the VPLMN, the UE shall select "urn:service:sos".

If the IP-CAN provided a local emergency number that matches the dialled number (see subclause 5.1.6.1), and:

- if the UE can derive one or more types of emergency service from the information received from the IP-CAN for the dialled number and the UE cannot derive types of emergency service from the information configured on the USIM for the dialled number; or
- if the UE is able to derive identical types of emergency service from both the information received from the IP-CAN for the dialled number and from the information configured on the USIM for the dialled number,

then the UE shall map any one of these emergency service types to an emergency service URN as specified in table B.2.2.6.1.

NOTE 3: How the UE resolves clashes where an emergency number is associated with one or more different types of emergency service configured in the USIM and in information received from the access network, is implementation dependent.

Upon reception of a 380 (Alternative Service) response to an INVITE request as defined in subclause 5.1.2A.1.1 and subclause 5.1.3.1, if:

- the 380 (Alternate Service) response contains a Contact header field;
- the value of the Contact header field is a service URN; and

- the service URN has a top-level service type of "sos";

then the UE determines that "emergency service information is included" as described 3GPP TS 23.167 [4B], else the UE determines that "emergency service information" as described 3GPP TS 23.167 [4B] is not included.

If the "emergency service information is included" as described 3GPP TS 23.167 [4B]:

- 1) if the URN in the Contact header field matches an emergency service URN in table B.2.2.6.1, then the type of emergency service is the value corresponding to the matching entry in table B.2.2.6.1; and
- 2) if the URN in the Contact header field does not match any emergency service URN in table B.2.2.6.1, then the type of emergency service is not identified.

NOTE 4: In bullet 2), the URN in the Contact header field either contains "no emergency subservice type" as described in 3GPP TS 23.167 [4B] triggering an emergency call, or contains an "emergency subservice type that does not map into an emergency service category for the CS domain" as described in 3GPP TS 23.167 [4B] triggering a normal call when the dialled number is available or triggering an emergency call when the dialled number is not available.

---

## B.2A Usage of SDP

### B.2A.0 General

NOTE: When:

- establishing a session which is not an emergency session; or
- modifying a session which is not an emergency session;

and if the IMSVoPS indicator is received in the "Network feature support" Information Element (see 3GPP TS 24.008 [8]), the UE constructs SDP based on the restrictions indicated in the IMSVoPS indicator. Regardless whether the IMSVoPS indicator indicating voice is supported or not, m-lines can be set to "audio" and exclude voice codecs from the SDP answer or SDP offer.

### B.2A.1 Impact on SDP offer / answer of activation or modification of PDP contexts for media by the network

If due to the activation of PDP context from the network the related SDP media description needs to be changed the UE shall update the related SDP information by sending a new SDP offer within a SIP request, which is sent over the existing SIP dialog,

If the UE receives a modification request from the network for a PDP context that is used for one or more media streams in an ongoing SIP session, the UE shall:

- 1) if, due to the modification of the PDP context, the related SDP media description need to be changed, update the related SDP information by sending a new SDP offer within a SIP request, that is sent over the existing SIP dialog, and respond to the PDP context modification request.

NOTE: The UE can decide to indicate additional media streams as well as additional or different codecs in the SDP offer than those used in the already ongoing session.

### B.2A.2 Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE

If the UE receives an SDP offer where the SDP offer includes all media streams for which the originating side indicated its local preconditions as met, if the precondition mechanism is supported by the terminating UE and the IP-CAN performs network-initiated resource reservation for the terminating UE and the available resources are not sufficient for the received offer the terminating UE shall indicate its local preconditions and provide the SDP answer to the originating side without waiting for resource reservation.

NOTE 1: If the resource reservation is controlled by the GPRS IP-CAN, the resource reservation request is initiated by the GGSN after the P-CSCF has authorised the respective IP flows and provided the QoS requirements over the Rx interface to the PCRF as described in 3GPP TS 29.214 [13D].

NOTE 2: During the PDP context activation procedure the UE and network negotiate whether the UE or the GPRS IP-CAN is responsible for the resource reservation applicable to all PDP contexts within the activated PDP address/APN pair as described in 3GPP TS 24.008 [8].

## B.2A.3 Emergency service

NOTE: When establishing an emergency session or when modifying an emergency session, the IMSVoPS indicator does not influence handling of SDP offer and SDP answer.

---

## B.3 Application usage of SIP

### B.3.1 Procedures at the UE

#### B.3.1.1 P-Access-Network-Info header field

The UE shall always include the P-Access-Network-Info header field where indicated in subclause 5.1.

#### B.3.1.2 Availability for calls

The UE indicates to the non-access stratum the status of being available for voice over PS when:

- 1) the UE is capable of receiving any (but not necessarily all) of the media types which the CS domain supports, such that the media type can also be used when accessing the IM CN subsystem using the current IP-CAN;
- 2) if the media type of item 1 is an "audio" media type, and the UE supports codecs suitable for (conversational) speech; and
- 3) the UE determines a contact has been bound to a public user identity using the IP-CAN, such that this contact is expected to be used for the delivery of incoming requests in the IM CN subsystem relating to such media.

The UE indicates to the non-access stratum the status of being not available for voice over PS when these conditions are no longer met.

#### B.3.1.2A Availability for SMS

The UE determines whether the UE is able to use SMS using IMS when the UE:

- I) is capable of using the MIME type "application/vnd.3gpp.sms" (see 3GPP TS 24.341 [8L]), such that the MIME type can also be used when accessing the IM CN subsystem using the current IP-CAN;
- II) supports the role of an SM-over-IP sender (see 3GPP TS 24.341 [8L]);
- IIA) determines the PDP context used for SIP signalling exists; and
- III) determines a contact has been bound to a public user identity using the IP-CAN, such that this contact is expected to be used for the delivery of incoming requests in the IM CN subsystem relating to such media.

When above criteria are not matched UE determines SMS using IMS is unavailable.

#### B.3.1.3 Authorization header field

Void.

### B.3.1.4 SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE

Upon receiving an INVITE request not including the "precondition" option-tag in the Supported header field and not including the "precondition" option-tag in the Require header field, and the IP-CAN performs network-initiated resource reservation for the UE, the UE:

- 1) if the INVITE request contains an SDP offer and the local resources required at the terminating UE for the received SDP offer are not available:
  - a) shall not alert the user; and
  - b) shall send 183 (Session Progress) response to the INVITE request without waiting for resource reservation and without alerting the user. If the INVITE request includes a Supported header field indicating support of reliable provisional responses, the UE shall send the 183 (Session Progress) response reliably. In the 183 (Session Progress) response, the UE shall include an SDP answer; and
- 2) if the INVITE request does not contain an SDP offer and the INVITE request includes a Supported header field indicating support of reliable provisional responses:
  - a) shall generate an SDP offer; and
  - b) if the local resources required at the terminating UE for the generated SDP offer are not available:
    - A) shall not alert the user; and
    - B) shall reliably send 183 (Session Progress) response to the INVITE request without waiting for resource reservation and without alerting the user. In the 183 (Session Progress) response, the UE shall include the generated SDP offer.

Upon successful reservation of local resources, if the precondition mechanism is not used by the terminating UE, the UE can send 180 (Ringing) response to the INVITE request and can alert the user.

## B.3.2 Procedures at the P-CSCF

### B.3.2.1 Determining network to which the originating user is attached

In order to determine from which network the request was originated the P-CSCF shall check the MCC and MNC fields received in the P-Access-Network-Info header field.

NOTE: The above check can be against more than one MNC code stored in the P-CSCF.

### B.3.2.2 Location information handling

Void.

### B.3.2.3 Prohibited usage of PDN connection for emergency bearer services

If the P-CSCF detects that a UE uses a PDN connection for emergency bearer services for a non-emergency REGISTER request, the P-CSCF shall reject that request by a 403 (Forbidden) response.

NOTE: By assigning specific IP address ranges for a PDN connection for emergency bearer services and configuring those ranges in P-CSCF, the P-CSCF can detect based on the registered Contact address if UE uses an emergency PDN connection for initial registration.

## B.3.3 Procedures at the S-CSCF

### B.3.3.1 Notification of AS about registration status

Not applicable

---

## B.4 3GPP specific encoding for SIP header field extensions

### B.4.1 Void

---

## B.5 Use of circuit-switched domain

When an emergency call is to be set up over the CS domain, the UE shall attempt it according to the procedures described in 3GPP TS 24.008 [8].

---

## Annex C (normative): UICC and USIM Aspects for access to the IM CN subsystem

### C.1 Scope

This clause describes the UICC and USIM aspects for access to the IM CN subsystem. Additional requirements related to UICC usage for access to the IM CN subsystem are described in 3GPP TS 33.203 [19].

---

### C.2 Derivation of IMS parameters from USIM

In case the UE is loaded with a UICC that contains a USIM but does not contain an ISIM, the UE shall:

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to.

All these three parameters are derived from the IMSI parameter in the USIM, according to the procedures described in 3GPP TS 23.003 [3]. Also in this case, the UE shall derive new values every time the UICC is changed, and shall discard existing values if the UICC is removed.

**NOTE:** If there is an ISIM and a USIM on a UICC, the ISIM is used for authentication to the IM CN subsystem, as described in 3GPP TS 33.203 [19]. See also subclause 5.1.1.1A.

---

### C.3 ISIM Location in 3GPP Systems

For 3GPP systems, if ISIM is present, it is contained in UICC.

---

#### C.3A UICC access to IMS

If the UE supports the UICC access to IMS USAT feature defined in 3GPP TS 31.111 [15D] the following procedures in addition to the UE procedures in this specification apply.

If the  $EF_{UICCIARI}$  contains a list of IARIs associated with active applications installed on the UICC in either the USIM or the ISIM, then when performing the user-initiated registration procedure as described in subclause 5.1.1.2 the UE shall include in the REGISTER request the list of IARIs associated with active applications installed on the UICC in addition to any IARI values for active applications installed on the ME in g.3gpp.iari-ref media feature tag(s) in the Contact header field of the REGISTER request as defined in subclause 7.9.3 and RFC 3840 [62].

If the UE receives from the UICC an initial request for a dialog or a standalone transaction then after decapsulating the request as specified in 3GPP TS 31.111 [15D] the UE shall send the request to the IM CN subsystem as specified in subclause 5.1.2A. When the UE receives from the UICC subsequent requests or responses related to dialogs or transactions already established for UICC applications then after decapsulating the request or response as specified in 3GPP TS 31.111 [15D] the UE shall send the request or response to the IM CN subsystem as specified in subclause 5.1.2A.

**NOTE:** The encapsulated requests and responses transferred between the UICC and UE are complete and valid SIP requests and responses compliant with RFC 3261 [26].

When sending requests or responses received from the UICC to the IM CN subsystem the UE shall modify or include any header fields necessary (such as Route, Via, Contact) in order to conform with the procedures in this specification.

---

## C.4 Update of IMS parameters on the UICC

3GPP TS 31.102 [15C] and 3GPP TS 31.103 [15B] specify the file structure and contents for the preconfigured parameters stored on the USIM and ISIM, respectively, necessary to initiate the registration to the IM CN subsystem. Any of these parameters can be updated via Data Download or a USAT application, as described in 3GPP TS 31.111 [15D]. If one or more EFs are changed and a REFRESH command is issued by the UICC, then the UE reads the updated parameters from the UICC as specified for the REFRESH command in 3GPP TS 31.111 [15D].

If the UE supports the UICC access to IMS USAT feature defined in 3GPP TS 31.111 [15D] and the EF<sub>UICCIARI</sub> changes in either the USIM or the ISIM, the UE shall perform the user-initiated reregistration procedure as described in subclause 5.1.1.4 with the new values of the IARI parameter(s) residing on the UICC.

In case of changes to EFs other than the EF<sub>UICCIARI</sub>, the UE is not required to perform deregistration but it shall wait for the network-initiated deregistration procedures to occur as described in subclause 5.4.1.5 unless the user initiates deregistration procedures as described in subclause 5.1.1.6. From this point onwards the normal initial registration procedures can occur.



---

## Annex D (normative): IP-Connectivity Access Network specific concepts when using I-WLAN to access IM CN subsystem

### D.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is Wireless LAN Interworking (I-WLAN).

---

### D.2 I-WLAN aspects when connected to the IM CN subsystem

#### D.2.1 Introduction

A WLAN UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by I-WLAN to provide packet-mode communication between the WLAN UE and the IM CN subsystem.

Requirements for the WLAN UE on the use of these packet-mode services are specified in this clause. Requirements for the PDG in support of this communication are specified in 3GPP TS 29.161 [11C]. When using the I-WLAN, the IP-CAN bearer is provided by an I-WLAN tunnel.

#### D.2.2 Procedures at the WLAN UE

##### D.2.2.1 I-WLAN tunnel activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the WLAN UE shall:

- a) perform I-WLAN network selection, i.e. gaining 3GPP Direct access as described in 3GPP TS 24.234 [8C] in the access dependent case;
- b) establish an IKEv2 security association and an IPsec ESP security association (I-WLAN tunnel) with the PDG according to the W-APN and PDG selection criteria described in 3GPP TS 24.234 [8C]. The IKEv2 security association and IPsec ESP security association (I-WLAN tunnel) shall remain active throughout the period the WLAN UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration.

The WLAN UE may carry both signalling and media on an IPsec ESP security association.

- c) Acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

- I. Use DHCP mechanism
- II. Use DNS

When using IPv4, the WLAN UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F]. When using IPv6, the WLAN UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C].

- III. Obtain the list of P-CSCF address(es) from the IMS management object

The WLAN UE can freely select method I, II, or III for P-CSCF discovery. If DHCP is used, the following procedures apply:

Upon establishing an IP-CAN, the WLAN UE may use the Dynamic Host Configuration Protocol (DHCP) specified in RFC 2131 [40A] or Dynamic Host Configuration Protocol for IPv6 (DHCPv6) specified in RFC 3315 [40] to discover the P-CSCF.

Prior to accessing the DHCP server, the WLAN UE will have obtained an IP address via means other than DHCP and DHCPv6.

If the WLAN UE uses DHCP for P-CSCF discovery and the WLAN UE is unaware of the address of the DHCP server, the WLAN UE shall send the DHCPINFORM using the limited broadcast IP address (i.e., 255.255.255.255) and UDP port 67. If the WLAN UE knows the IP address of the DHCP server, the WLAN UE shall send the DHCPINFORM to the DHCP server's unicast IP address and UDP port 67. The DHCP server sends the DHCPACK on the IP address specified in the Client IP Address field of the DHCPINFORM. The DHCP server may include, in the DHCPACK, the SIP Server DHCP Option specified in RFC 3361 [35A], which carries either a list of IPv4 address(es) of the P-CSCF(s) or a list of DNS fully qualified domain name(s) that can be mapped to one or more P-CSCF(s). If the WLAN UE uses DHCPv6 for P-CSCF discovery and the WLAN UE is unaware of the address of the DHCP Server, the WLAN UE shall send an Information Request using the IPv6 multicast address FF02::1:2 and the UDP port 547. If the WLAN UE knows the IP address of the DHCPv6 server, the WLAN UE shall send the Information Request message to the DHCPv6 server's IP address and UDP port 547. In the Information Request, the WLAN UE may request either one or both the SIP Servers Domain Name List option and the SIP Servers IPv6 Address List option specified in RFC 3319 [41]. The DHCP server sends the Reply to the IP address specified in the Information Request. The DHCP server may include in the Reply either one or both the SIP Servers Domain Name List option and the SIP Servers IPv6 Address List option, as requested by the WLAN UE.

In case several P-CSCF's IP addresses or domain names are provided to the WLAN UE, the WLAN UE shall perform P-CSCF selection according to RFC 3361 [35A] or RFC 3319 [41]. The WLAN UE shall perform the procedure for the resolution of domain name according to RFC 3263 [27A]. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the WLAN UE is implementation specific.

### D.2.2.1A Modification of a I-WLAN tunnel used for SIP signalling

Not applicable.

### D.2.2.1B Re-establishment of the I-WLAN tunnel used for SIP signalling

Not applicable.

### D.2.2.1C P-CSCF restoration procedure

A WLAN UE supporting the P-CSCF restoration procedure uses the keep-alive procedures described in RFC 6223 [143].

If the P-CSCF fails to respond to keep-alive requests the WLAN UE shall acquire a different P-CSCF address using any of the methods described in the subclause D.2.2.1 and perform an initial registration as specified in subclause 5.1.

#### D.2.2.2 Void

#### D.2.2.3 Void

#### D.2.2.4 Void

### D.2.2.5 I-WLAN tunnel procedures for media

#### D.2.2.5.1 General requirements

The WLAN UE can establish media streams that belong to different SIP sessions on the same I-WLAN tunnel.

During establishment of a session, the WLAN UE establishes data streams(s) for media related to the session. Such data stream(s) may result in activation of additional IPsec ESP security associations (I-WLAN tunnels).

If the WLAN UE receives indication within the SDP according to RFC 3524 [54] that media stream(s) belong to group(s), the media stream(s) shall be set up on separate IPsec ESP security associations (I-WLAN tunnels) according

to the indication of grouping of media streams. The WLAN UE may freely group media streams to IPsec ESP security association (I-WLAN tunnel(s)) in case no indication of grouping of media streams is received from the P-CSCF.

If the capabilities of the originating WLAN UE, or operator policy at the PDG prevents the originating WLAN UE from establishment of additional IPsec ESP security associations (I-WLAN tunnels) according to the media grouping attributes given by the P-CSCF in accordance with RFC 3524 [54], the WLAN UE will not establish such grouping of media streams. Instead, the originating WLAN UE shall negotiate media parameters for the session according to RFC 3264 [27B].

If the capabilities of the terminating WLAN UE or operator policy at the PDG prevents the originating WLAN UE from establishment of additional IPsec ESP security associations (I-WLAN tunnels) according to the media grouping attributes given by the P-CSCF in accordance with RFC 3524 [54], the WLAN UE will not establish such grouping of media streams. Instead, the terminating WLAN UE shall handle such SDP offers in accordance with RFC 3388 [53].

The WLAN UE can receive a media authorization token in the P-Media-Authorization header field from the P-CSCF according to RFC 3313 [31]. If a media authorization token is received in the P-Media-Authorization header field when a SIP session is initiated, the WLAN UE shall reuse the existing I-WLAN tunnel and ignore the media authorization token.

#### D.2.2.5.1A Activation or modification of I-WLAN tunnel for media by the WLAN UE

Not applicable.

#### D.2.2.5.1B Activation or modification of I-WLAN tunnel for media by the network

Not applicable.

#### D.2.2.5.1C Deactivation of I-WLAN tunnel for media

Not applicable.

#### D.2.2.5.2 Special requirements applying to forked responses

Since the WLAN UE is unable to perform bearer modification, forked responses place no special requirements on the WLAN UE.

#### D.2.2.5.3 Unsuccessful situations

Not applicable.

#### D.2.2.6 Emergency service

The details of network selection to select HPLMN or VPLMN are specified in 3GPP TS 24.234 [8C].

The WLAN UE may reuse an existing I-WLAN tunnel for the purpose of making an IMS emergency call only if the WLAN UE is not roaming (i.e. not accessing via a VPLMN) as described in 3GPP TS 24.234 [8C].

---

## D.2A Usage of SDP

### D.2A.0 General

Not applicable.

### D.2A.1 Impact on SDP offer / answer of activation or modification of I-WLAN tunnel for media by the network

Not applicable.

## D.2A.2 Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE

Not applicable.

## D.2A.3 Emergency service

No additional procedures defined.

---

# D.3 Application usage of SIP

## D.3.1 Procedures at the UE

### D.3.1.1 P-Access-Network-Info header field

The UE shall always include the P-Access-Network-Info header field where indicated in subclause 5.1.

### D.3.1.2 Availability for calls

Not applicable.

#### D.3.1.2A Availability for SMS

Void.

### D.3.1.3 Authorization header field

Void.

### D.3.1.4 SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE

Not applicable.

## D.3.2 Procedures at the P-CSCF

### D.3.2.1 Determining network to which the originating user is attached

NOTE: Determining the network to which the originating user is attached is not specified.

### D.3.2.2 Location information handling

Void.

## D.3.3 Procedures at the S-CSCF

### D.3.3.1 Notification of AS about registration status

Not applicable

---

## D.4 3GPP specific encoding for SIP header field extensions

Void.

---

## D.5 Use of circuit-switched domain

Void.

---

# Annex E (normative): IP-Connectivity Access Network specific concepts when using xDSL, Fiber or Ethernet to access IM CN subsystem

## E.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is xDSL, Fiber or Ethernet.

NOTE: Fixed-broadband access in this Annex refers to xDSL, Fiber and Ethernet accesses.

---

## E.2 Fixed broadband aspects when connected to the IM CN subsystem

### E.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by the fixed-broadband access network to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the IP Edge node, defined in ETSI ES 282 001 [138] in support of this communication are outside the scope of this document and specified elsewhere.

From the UEs perspective, it is assumed that one or more IP-CAN bearer(s) are provided, in the form of connection(s) managed by the layer 2 (e.g. DSL modem supporting the UE).

In the first instance, it is assumed that the IP-CAN bearer(s) is (are) statically provisioned between the UE and the IP Edge node, defined in ETSI ES 282 001 [138], according to the user's subscription.

It is out of the scope of the current Release to specify whether a single IP-CAN bearer is used to convey both signalling and media flows, or whether several PVC connections are used to isolate various types of IP flows (signalling flows, conversational media, non conversational media...).

The end-to-end characteristics of the fixed-broadband IP-CAN bearer depend on the type of access network, and on network configuration. The description of the network PVC termination (e.g., located in the DSLAM, in the BRAS...) is out of the scope of this annex.

### E.2.2 Procedures at the UE

#### E.2.2.1 Activation and P-CSCF discovery

Fixed-broadband bearer(s) is (are) statically provisioned in the current Release.

Unless a static IP address is allocated to the UE, prior to communication with the IM CN subsystem, the UE shall perform a Network Attachment procedure depending on the used fixed-broadband access type. When using a fixed-broadband access, both IPv4 and IPv6 UEs may access the IM CN subsystem. The UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or a DNS Server IPv6 address(es) via RFC 3315 [40].

The methods for P-CSCF discovery are:

- I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1. In case the DHCP server provides several P-CSCF addresses or FQDNs to the UE, the UE shall select the P-CSCF address or FQDN as indicated in RFC 3319 [41]. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

II. The UE selects a P-CSCF from the list in the IMS management object as specified in 3GPP TS 24.167 [8G].

The UE shall use method II to select a P-CSCF if the IMS management object contains the P-CSCF list. Otherwise, the UE shall use method I to select a P-CSCF.

### E.2.2.1A Modification of a fixed-broadband connection used for SIP signalling

Not applicable.

### E.2.2.1B Re-establishment of a fixed-broadband connection used for SIP signalling

Not applicable.

### E.2.2.1C P-CSCF restoration procedure

A UE supporting the P-CSCF restoration procedure uses the keep-alive procedures described in RFC 6223 [143].

If the P-CSCF fails to respond to keep-alive requests the UE shall acquire a different P-CSCF address using any of the methods described in the subclause E.2.2.1 and perform an initial registration as specified in subclause 5.1.

### E.2.2.2 Void

### E.2.2.3 Void

### E.2.2.4 Void

### E.2.2.5 Fixed-broadband bearer(s) for media

#### E.2.2.5.1 General requirements

The UE can establish media streams that belong to different SIP sessions on the same fixed-broadband bearer.

#### E.2.2.5.1A Activation or modification of fixed-broadband bearers for media by the UE

If the UE receives indication within the SDP according to RFC 3524 [54] that media stream(s) belong to group(s), and if several fixed-broadband bearers are available to the UE for the session, the media stream(s) may be sent on separate fixed-broadband bearers according to the indication of grouping. The UE may freely group media streams to fixed-broadband bearers in case no indication of grouping is received from the P-CSCF.

If the UE receives media grouping attributes in accordance with RFC 3524 [54] that it cannot provide within the available fixed-broadband bearer(s), then the UE shall handle such SDP offers in accordance with RFC 3388 [53].

The UE can receive a media authorization token in the P-Media-Authorization header field from the P-CSCF according to RFC 3313 [31]. If a media authorization token is received in the P-Media-Authorization header field when a SIP session is initiated, the UE shall reuse the existing fixed-broadband bearer(s) and ignore the media authorization token.

#### E.2.2.5.1B Activation or modification of fixed-broadband bearers for media by the network

Not applicable.

#### E.2.2.5.1C Deactivation of fixed-broadband bearers for media

Not applicable.

#### E.2.2.5.2 Special requirements applying to forked responses

Since the UE is unable to perform bearer modification, forked responses place no special requirements on the UE.

#### E.2.2.5.3 Unsuccessful situations

Not applicable.

## E.2.2.6 Emergency service

If attached to network via fixed-broadband access technology, the UE shall always consider being attached to its home operator's network for the purpose of emergency calls.

NOTE: In fixed-broadband the UE is unable to receive any indication from the network, that would allow the UE to determine, whether it is currently attached to its home operator's network or to a different network, so the UE assumes itself always attached to the home operator's network when connected via fixed-broadband access technology.

---

## E.2A Usage of SDP

### E.2A.0 General

Not applicable.

### E.2A.1 Impact on SDP offer / answer of activation or modification of xDSL bearer for media by the network

Not applicable.

### E.2A.2 Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE

Not applicable.

### E.2A.3 Emergency service

No additional procedures defined.

---

## E.3 Application usage of SIP

### E.3.1 Procedures at the UE

#### E.3.1.1 P-Access-Network-Info header field

The UE may, but need not, include the P-Access-Network-Info header field where indicated in subclause 5.1.

#### E.3.1.2 Availability for calls

Not applicable.

#### E.3.1.2A Availability for SMS

Void.

#### E.3.1.3 Authorization header field

When using SIP digest or SIP digest without TLS, the UE need not include an Authorization header field on sending a REGISTER request, as defined in subclause 5.1.1.2.1.



NOTE: In case the Authorization header field is absent, the mechanism only supports that one public user identity is associated with only one private user identity. The public user identity is set so that it is possible to derive the private user identity from the public user identity by removing SIP URI scheme and the following parts of the SIP URI if present: port number, URI parameters, and To header field parameters. Therefore, the public user identity used for registration in this case cannot be shared across multiple UEs. Deployment scenarios that require public user identities to be shared across multiple UEs that don't include an private user identity in the initial REGISTER request can be supported as follows:

- Assign each sharing UE a unique public user identity to be used for registration,
- Assign the shared public user identities to the implicit registration set of the unique registering public user identities assigned to each sharing UE.

#### E.3.1.4 SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE

Not applicable.

### E.3.2 Procedures at the P-CSCF

#### E.3.2.1 Determining network to which the originating user is attached

In order to determine from which network the request was originated the P-CSCF shall check if the location information received in the network provided and/or UE provided "dsl-location", "eth-location" or "fiber-location" parameter in the P-Access-Network-Info header field(s) belongs to a location in the same country.

NOTE 1: If local policy does not require the insertion of P-Access-Network-Info header field in the P-CSCF even if it is missing in the received initial request, the P-CSCF can assume that the request is initiated by fixed broadband UE in the same country.

NOTE 2: If the location information in the network provided and UE provided "dsl-location", "eth-location" or "fiber-location" parameters (in a request that includes two P-Access-Network-Info header fields) is contradictory, or the two P-Access-Network-Info header fields indicate different access types the P-CSCF ignores either the network provided or the UE provided information according to operator policy.

#### E.3.2.2 Location information handling

Upon receipt of an initial request for a dialog or standalone transaction or an unknown method, the P-CSCF based on local policy may include a P-Access-Network-Info header field. The value of the "dsl-location", "eth-location" or "fiber-location" parameter shall be the value as received in the Location-Information header in the User-Data Answer command as specified in ETSI ES 283 035 [98].

NOTE: The way the P-CSCF deduce that the request comes from a UE connected through xDSL access is implementation dependent.

### E.3.3 Procedures at the S-CSCF

#### E.3.3.1 Notification of AS about registration status

Not applicable

---

## E.4 3GPP specific encoding for SIP header field extensions

Void.

---

## E.5 Use of circuit-switched domain

There is CS domain in this access technology.

---

## Annex F (normative): Additional procedures in support for hosted NAT

NOTE: This subclause describes the mechanism for support of the hosted NAT scenario. This does not preclude other mechanisms but they are out of the scope of this annex.

---

### F.1 Scope

This annex describes the UE and P-CSCF procedures in support of hosted NAT. In this scenario, both the media flows and the SIP signalling both traverse a NA(P)T device located in the customer premises domain. The term "hosted NAT" is used to address this function.

When receiving an initial SIP REGISTER request without integrity protection, the P-CSCF can, determine whether to perform the hosted NAT procedures for the user identified by the REGISTER request by comparing the address information in the top-most SIP Via header field with the IP level address information from where the request was received. The P-CSCF will use the hosted NAT procedure only when the address information do not match.

NOTE: There is no need for the P-CSCF to resolve a domain name in the Via header field when UDP encapsulated tunnel mode for IPsec is used. The resolution of a domain name in the Via header field is not required by RFC 3261 [26].

In order to provide hosted NAT traversal for SIP REGISTER requests without integrity protection and the associated responses, the P-CSCF makes use of the "received" and "rport" header field parameters as described in RFC 3261 [26] and RFC 3581 [56A]. The hosted NAT traversal for protected SIP messages is provided by applying UDP encapsulation to IPsec packets in accordance with RFC 3948 [63A].

Alternatively to the procedures defined in subclause F.2 which are employed to support the hosted NAT scenario where the security solution is based on UDP encapsulated IPsec as defined in 3GPP TS 33.203 [19], subclause F.4 provides procedures for NAT traversal for security solutions that are not defined in 3GPP TS 33.203 [19]. Use of such security solutions is outside the scope of this document.

---

### F.2 Application usage of SIP

#### F.2.1 UE usage of SIP

##### F.2.1.1 General

This subclause describes the UE SIP procedures for supporting hosted NAT scenarios. The description enhances the procedures specified in subclause 5.1.

The UE shall support the symmetric response routing mechanism according to RFC 3581 [56A].

##### F.2.1.2 Registration and authentication

###### F.2.1.2.1 General

The text in subclause 5.1.1.1 applies without changes

###### F.2.1.2.1A Parameters contained in the ISIM

The text in subclause 5.1.1.1A applies without changes

###### F.2.1.2.1B Parameters provisioned to a UE without ISIM or USIM

The text in subclause 5.1.1.1B applies without changes.

###### F.2.1.2.2 Initial registration

The procedures described in subclause 5.1.1.2.1 apply with the additional procedures described in the present subclause.

NOTE 1: In accordance with the definitions given in subclause 3.1 the IP address acquired initially by the UE in a hosted NAT scenario is the UE private IP address.

On sending a REGISTER request, the UE shall populate the header fields as indicated in subclause 5.1.1.2.1 with the exceptions of subitems c) and d) which are modified as follows

The UE shall populate:

- c) a Contact header field according to the following rules: if the REGISTER request is sent without integrity protection, the Contact header field shall be set to include SIP URI(s) containing the private IP address of the UE in the hostport parameter or FQDN. If the UE supports GRUU, the UE shall include a "+sip.instance" header field parameter containing the instance ID. If the REGISTER request is integrity protected, the UE shall include the public IP address or FQDN in the hostport parameter. The UE shall only use a FQDN in a protected REGISTER request, if it is ensured that the FQDN resolves to the public IP address of the NAT. If the UE supports GRUU, the UE shall include a "+sip.instance" header field parameter containing the instance ID. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];

NOTE 2: The UE will learn its public IP address from the "received" header field parameter in the topmost Via header field in the 401 (Unauthorized) response to the unprotected REGISTER request.

- d) a Via header field according to the following rules: if the REGISTER request is sent without integrity protection, the Via header field shall be set to include the private IP address or FQDN of the UE in the sent-by field. If the REGISTER request is integrity protected, the UE shall include the public IP address or FQDN in the sent-by field. The UE shall only use a FQDN in a protected REGISTER request, if it is ensured that the FQDN resolves to the public IP address of the NAT. Unless the UE has been configured to not send keep-alives, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with, the registration, as described in RFC 6223 [143];

NOTE 3: If the UE specifies a FQDN in the host parameter in the Contact header field and in the sent-by field in the Via header field of an unprotected REGISTER request, this FQDN will not be subject to any processing by the P-CSCF or other entities within the IM CN subsystem. The means to ensure that the FQDN resolves to the public IP address of the NAT are outside of the scope of this specification. One option for resolving this is local configuration.

If IMS AKA is used as a security mechanism, on sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as defined in subclause 5.1.1.2.2, with the exceptions of subitems c), and d) which are modified as follows:

- d) the Security-Client header field set to specify the security mechanisms the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the IPsec layer algorithms for integrity protection and for encryption as defined in 3GPP TS 33.203 [19], and shall announce support for them according to the procedures defined in RFC 3329 [48]. In addition to transport mode the UE shall support UDP encapsulated tunnel mode as per RFC 3948 [63A] and shall announce support for both modes as described in TS 33.203 [19];

When a 401 (Unauthorized) response to a REGISTER is received and this response is received without integrity protection, the procedures described in subclause 5.1.1.2.1 apply with the following additions:

The UE shall compare the values in the "received" header field parameter and "rport" header field parameter with the corresponding values in the sent-by parameter in the topmost Via header field to detect if the UE is behind a NAT. If the comparison indicates that the respective values are the same, the UE concludes that it is not behind a NAT.

- If the UE is not behind a NAT, the UE shall proceed with the procedures described in subclause 5.1 of the main body of this specification;
- If the UE is behind a NAT, the UE shall verify using the Security-Server header field that mode "UDP-enc-tun" is selected. If the verification succeeds the UE shall store the IP address contained in the "received" header field parameter as the UE public IP address. If the verification does not succeed the UE shall abort the registration.

In addition, when a 401 (Unauthorized) response to a REGISTER is received (with or without integrity protection) the UE shall behave as described in subclause F.2.1.2.5.

When the UE, that is behind a NAT, receives a 400 (Bad Request) response with 301 Warning header field indicating "incompatible network address format" to the unprotected REGISTER request, the UE shall randomly select new values for the protected server port and the protected client port, and perform new initiate registration procedure by sending an unprotected REGISTER request containing the new values in the Security-Client header field.

**Editor's Note:** [GINI CR#3968] The impact of bulk number registration procedures according to RFC 6140 [191] on the additional procedures in support for hosted NAT is FFS.

### F.2.1.2.3 Initial subscription to the registration-state event package

The procedures described in subclause 5.1.1.3 apply with the additional procedures described in subclause F.2.1.4.1.

### F.2.1.2.4 User-initiated re-registration

The procedures described in subclause 5.1.1.4.1 apply with the additional procedures described in the present subclause.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as indicated in subclause 5.1.1.4.1 with the exception of subitems c) and d) which are modified as follows.

The UE shall populate:

- c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the public IP address of the UE or FQDN, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];
- d) a Via header field set to include the public IP address or FQDN of the UE in the sent-by field. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continuous support to send keep-alives, as described in RFC 6223 [143];

NOTE 1: The means to ensure that the FQDN resolves to the public IP address of the NAT are outside of the scope of this specification. One option for resolving this is local configuration.

When the UE, that is behind a NAT, receives a 400 (Bad Request) response with 301 Warning header field indicating "incompatible network address format" to the REGISTER request that does not contain a challenge response, the UE shall randomly select a new value for the protected client port, and send the REGISTER request containing the new values in the Security-Client header field.

NOTE 2: The protected server port stays fixed for a UE until all public user identities of the UE have been de-registered.

**Editor's Note:** [GINI CR#3968] The impact of bulk number registration procedures according to RFC 6140 [191] on the additional procedures in support for hosted NAT is FFS.

### F.2.1.2.5 Authentication

#### F.2.1.2.5.1 IMS AKA - general

The procedures of subclause 5.1.1.5.1 apply with with the additional procedures described in the present subclause.

On receiving a 401 (Unauthorized) response to the REGISTER request and the response is deemed to be valid, the UE shall behave as of subclause 5.1.1.5.1 with the exception of subitem 3) which is modified as follows.

The UE shall:

- 3) send another REGISTER request using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial request (see subclause F.2.1.2.2), with the addition that the UE shall include an Authorization header field containing the private user identity and the authentication challenge response calculated by the UE using RES and other parameters, as described in RFC 3310 [49]. The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the integrity protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

Whenever the 200 (OK) response is not received before the temporary SIP level lifetime of the temporary set of security associations expires or a 403 (Forbidden) response is received, the UE shall consider the registration to have failed. The UE shall delete the temporary set of security associations it was trying to establish, and use the old set of security associations. The UE should send an unprotected REGISTER request according to the procedure specified in subclause F.2.1.2.2 if the UE considers the old set of security associations to be no longer active at the P-CSCF.

#### F.2.1.2.5.2 Void

#### F.2.1.2.5.3 IMS AKA abnormal cases

The text in subclause 5.1.1.5.3 applies without changes.

#### F.2.1.2.5.4 SIP digest – general

Not applicable.

#### F.2.1.2.5.5 SIP digest – abnormal procedures

Not applicable.

#### F.2.1.2.5.6 SIP digest with TLS – general

Not applicable.

#### F.2.1.2.5.7 SIP digest with TLS – abnormal procedures

Not applicable.

#### F.2.1.2.5.8 Abnormal procedures for all security mechanisms

The text in subclause 5.1.1.5.8 applies without changes.

#### F.2.1.2.5A Network-initiated re-authentication

The text in subclause 5.1.1.5A applies without changes.

#### F.2.1.2.5B Change of IPv6 address due to privacy

The text in subclause 5.1.1.5B applies without changes.

#### F.2.1.2.6 User-initiated deregistration

The procedures of subclause 5.1.1.6.1 apply with with the additional procedures described in the present subclause.

On sending a REGISTER request, the UE shall populate the header fields as indicated in subclause 5.1.1.6 with the exception of subitems d) and e) which are modified as follows.

The UE shall populate:

- c) a Contact header field set to either the value of "\*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN; and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT;
- d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT;

NOTE 1: In case of hosted NAT traversal only the UE public IP addresses are bound to security associations.

NOTE 2: The means to ensure that the FQDN resolves to the public IP address of the NAT are outside of the scope of this specification. One option for resolving this is local configuration.

**Editor's Note: [GINI CR#3968] The impact of bulk number registration procedures according to RFC 6140 [191] on the additional procedures in support for hosted NAT is FFS.**

### F.2.1.2.7 Network-initiated deregistration

The procedures of subclause 5.1.1.7 apply with with the additional procedures described in the present subclause.

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) which were registered by this UE with:

- the state attribute set to "terminated" and the event attribute set to "rejected" or "deactivated"; or
- the state attribute set to "active" and the state attribute within the <contact> element belonging to this UE set to "terminated", and associated event attribute element to "rejected" or "deactivated";

the UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the initial registration procedure as described in subclause F.2.1.2.2. In case of a "rejected" event attribute, the UE shall release all dialogs related to those public user identities.

### F.2.1.3 Subscription and notification

The text in subclause 5.1.2 applies without changes.

### F.2.1.4 Generic procedures applicable to all methods excluding the REGISTER method

#### F.2.1.4.1 UE originating case

The procedures described in subclause 5.1.2A.1 apply with the additional procedures described in the present subclause.

When the UE sends any request, the requirements in subclause 5.1.2A.1 are replaced by the following requirements. The UE shall include:

- a Via header field set to include the public IP address of the UE or FQDN and the protected server port in the sent-by field. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT; and if this is a request for a new dialog, and the request includes a Contact header field, then the UE should populate the Contact header field as follows:
  - 1) if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does not indicate privacy of the P-Asserted-Identity, then insert the public GRUU ("pub-gruu" header field parameter) value in the Contact header field as specified in RFC 5627 [93]; or
  - 2) if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does indicate privacy of the P-Asserted-Identity, then insert the temporary GRUU ("temp-gruu" header field parameter) value in the Contact header field as specified in RFC 5627 [93].

If this is a request within an existing dialog, and the request includes a Contact header field, and the contact address previously used in the dialog was a GRUU, then the UE should insert the previously used GRUU value in the Contact header field as specified in RFC 5627 [93].

If the UE did not insert a GRUU in the Contact header field, then the UE shall include the public IP address of the UE or FQDN and the protected server port in the hostport parameter in any Contact header field that is otherwise included. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT.

**NOTE:** The means to ensure that the FQDN resolves to the public IP address of the NAT are outside of the scope of this specification. One option for resolving this is local configuration.

The UE shall discard any SIP response that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause F.2.1.2.4.

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause F.2.1.2.3.

#### F.2.1.4.2 UE terminating case

The procedures described in subclause 5.1.2A.2 apply with the additional procedures described in the present subclause.

When the UE sends any response, the requirements in subclause 5.1.2A.1 are replaced by the following requirement.

If the response includes a Contact header field, and the response is not sent within an existing dialog, then the UE should populate the Contact header field as follows:

- 1) if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity from the P-Called-Party-ID header field, and the UE does not indicate privacy of the P-Asserted-Identity, then insert the public GRUU ("pub-gruu" header field parameter) value in the Contact header field as specified in RFC 5627 [93]; and
- 2) if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity from the P-Called-Party-ID header field, and the UE does indicate privacy of the P-Asserted-Identity, then the UE should insert the temporary GRUU ("temp-gruu" header field parameter) value in the Contact header field as specified in RFC 5627 [93].

If the UE did not insert a GRUU in the Contact header field, then the UE shall:

- include the public IP address of the UE or FQDN and the protected server port in the hostport parameter in any Contact header field that is otherwise included. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT.

**NOTE:** The means to ensure that the FQDN resolves to the public IP address of the NAT are outside of the scope of this specification. One option for resolving this is local configuration.

The UE shall discard any SIP request that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause F.2.1.2.

## F.2.2 P-CSCF usage of SIP

### F.2.2.1 Introduction

This subclause describes the SIP procedures for supporting hosted NAT scenarios.

The description enhances the procedures specified in subclause 5.2.

The P-CSCF shall support the symmetric response routing mechanism according to RFC 3581 [56A].

**NOTE:** Symmetric response routing is used to support hosted NAT and applicable only to initial, unprotected REGISTER requests and corresponding responses.

### F.2.2.2 Registration

The procedures described in subclause 5.2.2 apply with the additional procedures described in the present subclause.

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall behave as of subclause 5.2.2.1.



If IMS AKA is the security mechanism, when the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall perform the procedures of subclause 5.2.2.2 with the following exception to items 2) and 3):

2) in case the REGISTER request was received without integrity protection, then:

- a) check the existence of the Security-Client header field. If the Security-Client header field is not present, then the P-CSCF shall return a suitable 4xx response. If the Security-Client header field is present the P-CSCF shall:
  - in case the UE indicated support for "UDP-enc-tun" then remove and store it.
  - in case the UE does not indicate support for "UDP-enc-tun" then:
    - if the host portion of the sent-by field in the topmost Via header field contains an IP address that differs from the source address of the IP packet, silently drop the REGISTER;
    - otherwise continue with procedures as of subclause 5.2.2.

NOTE 1: If the UE does not indicate support for "UDP-enc-tun" and the P-CSCF detects that the UE is located behind a NAT device, then the P-CSCF can just drop the REGISTER to avoid unnecessary signalling traffic.

- b) if the host portion of the sent-by field in the topmost Via header field contains a FQDN, or if it contains an IP address that differs from the source address of the IP packet, the P-CSCF shall:
  - add a "received" header field parameter in accordance with the procedure defined in RFC 3581 [56A]. The P-CSCF shall also set the value of the "rport" header field parameter to the source port of the request in accordance with the procedure defined in RFC 3581 [56A]; and
  - check that no any previously registered UE has either the same public IP address (allocated by the NAT and indicated in the Via header field) and the protected server port (specified in the Security-Client header field) or the same public IP address and the protected client port (specified in the Security-Client header field). If there is such UE, the P-CSCF shall return a 400 (Bad Request) response with 301 Warning header field indicating "incompatible network address format" to the unprotected REGISTER request. Otherwise, the P-CSCF shall forward the REGISTER request.

NOTE 2: If two UEs are behind the same NAT, the NAT can assign to them the same public IP address (but different NAT's port). Hence, the two respective UE must have different protected server port numbers, and different protected client port numbers.

3) in case the REGISTER request was received integrity protected, then the P-CSCF shall:

- a) check the security association which protected the request. If the security association is a temporary one, the P-CSCF shall:
  - in case the host parameter in the Contact address is in the form of a FQDN, ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address bound to the security association;
  - in case the P-CSCF has detected earlier that the UE is located behind a NAT, retrieve port\_Uenc from the encapsulating UDP header of the packet received and complete configuration of the temporary set of security associations by configuring port\_Uenc in each of the temporary security associations;
  - check whether the request contains a Security-Verify header field in addition to a Security-Client header field. If there are no such header fields, then the P-CSCF shall return a suitable 4xx response. If there are such header fields, then the P-CSCF shall compare the content of the Security-Verify header field with the content of the Security-Server header field sent earlier and the content of the Security-Client header field with the content of the Security-Client header field received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header field;
- b) if the security association the REGISTER request was received on, is an already established one, then the P-CSCF shall:
  - remove the Security-Verify header field if it is present;

- check if the Security-Client header field containing new parameter values is present, and:
- if this header field or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response.
- if this header field and the required parameters are present, then the P-CSCF shall check that no any previously registered UE has the same public IP address and the protected client port (specified in the Security-Client header field). If there is such UE, the P-CSCF shall return a 400 (Bad Request) response with 301 Warning header field indicating "incompatible network address format" to the REGISTER request. Otherwise, the P-CSCF shall remove and store the Security-Client header field before forwarding the request to the S-CSCF;

NOTE 3: When sending the protected REGISTER request to the P-CSCF, the UE will not modify the protected server port value, since the protected server port value stays fixed for a UE until all public user identities of the UE have been de-registered.

When the P-CSCF receives a 401 (Unauthorized) response to an unprotected REGISTER request and this response contains a "received" header field parameter and "rport" header field parameter in the Via header field associated with the UE and the UE indicated support for "UDP-enc-tun" IPsec mode, the P-CSCF shall:

- 1) delete any temporary set of security associations established towards the UE;
- 2) remove the "ck" and "ik" WWW-Authenticate header field parameters contained in the 401 (Unauthorized) response and bind the values to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the "ck" and "ik" header field parameters have been removed;
- 3) insert a Security-Server header field in the response, containing the P-CSCF security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the IPsec layer algorithms for integrity protection and for encryption as defined in 3GPP TS 33.203 [19]. The P-CSCF shall indicate "UDP-enc-tun" as the only IPsec mode;
- 4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. The P-CSCF shall select UDP encapsulated tunnel mode and shall leave the value for port-Uenc unspecified in each of the temporary security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and
- 5) send the 401 (Unauthorized) response unprotected to the UE using the mechanisms described in RFC 3261 [26] and RFC 3581 [56A], i.e. in case UDP is used as transport protocol the P-CSCF shall send the response to the IP address indicated in the "received" header field parameter and to the port indicated in the "rport" header field parameter of the Via header field associated with the UE. In case UDP is used as transport protocol, the P-CSCF shall use the IP address and the port on which the REGISTER request was received as source IP address and the source port when sending the response back to the UE.

When the P-CSCF receives a 401 (Unauthorized) response to a protected REGISTER request and that REGISTER request was protected by an old set of security associations that use UDP encapsulated tunnel mode, the P-CSCF shall:

- 1) delete any temporary set of security associations established towards the UE;
- 2) remove the "ck" and "ik" WWW-Authenticate header field parameters contained in the 401 (Unauthorized) response and bind the values to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the "ck" and "ik" header field parameters have been removed;
- 3) insert a Security-Server header field in the response, containing the P-CSCF security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the IPsec layer algorithms for integrity protection and encryption as defined in 3GPP TS 33.203 [19]. The P-CSCF shall indicate "UDP-enc-tun" as the IPsec mode;
- 4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. The P-CSCF shall select UDP encapsulated tunnel mode and shall specify the same port\_Uenc that was used in the old set of security associations. The P-CSCF

shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and

- 5) send the 401 (Unauthorized) response to the UE using the old set of security associations.

Otherwise, when the P-CSCF receives a 401 (Unauthorized) response to an unprotected REGISTER request and this response does not contain a "received" header field parameter and "rport" header field parameter or when the P-CSCF receives a 401 (Unauthorized) response to a protected REGISTER request and that REGISTER request was protected by an old set of security associations that do not use UDP encapsulated tunnel mode, the P-CSCF shall proceed as described in subclause 5.2.2.2.

## F.2.3 S-CSCF usage of SIP

### F.2.3.1 S-CSCF usage of SIP

#### F.2.3.1.1 Protected REGISTER with IMS AKA as a security mechanism

The procedures at the S-CSCF described in subclause 5.4.1.2.2 apply.

**NOTE:** When two UEs that are behind the same NAT register their contact addresses, the NAT can assign to them the same public IP address (but different NAT's ports). If these two UEs select the same protected server port number, and register via different P-CSCFs, then they will have the same contact addresses (i.e. same IP address and protected server port). However, any request targeted to either UE will be sent to the respective P-CSCF, hence not causing any ambiguity at the P-CSCF when forwarding the request via NAT.

---

## F.3 Void

## F.4 P-CSCF usage of SIP in case UDP encapsulated IPsec is not employed

### F.4.1 Introduction

The subclause F.4 describes the SIP procedures for supporting hosted NAT scenarios in case UDP encapsulated IPsec is not employed. In these scenarios the procedures for NAT traversal must take into account that all SIP requests and responses are not protected by an IPsec security association. This subclause also assumes that the UE transmits the SIP messages from the same IP address and port on which the UE expects to receive SIP messages. In addition, the procedures described in the present clause apply when the registration procedure as described in RFC 5626 [92] is not employed.

### F.4.2 Registration

The procedures described in subclause 5.2.2 apply with the additional procedures described in the present clause.

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall add the "received" header field parameter to the Via header field set to the source IP address of the packet header in accordance with the procedure defined in RFC 3261 [26] and RFC 3581 [56A]. The P-CSCF shall also set the value of the "rport" header field parameter to the source port of the request, in accordance with the procedure defined in RFC 3581 [56A].

When the P-CSCF detects that the UE is behind a NAT, and the UE has indicated support of the keep-alive mechanism defined in RFC 6223 [143], the P-CSCF shall indicate to the UE that it supports the keep-alive mechanism.

If, upon receiving a REGISTER request from an unregistered user and the P-CSCF discovers that the UE is behind a NAT, the P-CSCF performs the following actions on the Contact header field depending on its content:

- if the Contact header field contains a contact address in the form of an IP address (NOTE), the P-CSCF shall save (for the duration of the registration) this IP address (i.e. the private IP address of the UE) and associated port number (i.e. the private port of the UE) and bind them to the source IP address (i.e. the public IP address of the NAT) and the source port number (i.e. the port number of the NAT) of the IP packet that contained the REGISTER request and forward the REGISTER request;

- if the Contact header field contains more than one contact addresses in the form of an IP address, the P-CSCF shall apply the above procedure to one of those contact addresses by choosing the one with the highest qvalue parameter) and delete any other contact addresses containing an IP address. If the P-CSCF was unable to choose a contact address based on the qvalue, the P-CSCF shall choose one based on local policy and delete any other contact addresses containing an IP address.

NOTE: When the host parameter in the Contact address is in the form of a FQDN, the P-CSCF will resolve the given FQDN (by DNS lookup) to the IP address of the UE. When including the FQDN in the Contact header field the UE insures that the FQDN resolves to the IP address that the UE uses to send the REGISTER request.

When the P-CSCF received a response to the above request, the P-CSCF shall forward the response to the UE using the mechanisms described in RFC 3581 [56A]. In case UDP is used, the P-CSCF shall send the response to the IP address indicated in the "received" header field parameter and to the port indicated in the "rport" header field parameter of the Via header field in the response. If the REGISTER request received from the UE was received over a TCP connection, the P-CSCF shall send the response to the UE over the same TCP connection over which the request was received. The P-CSCF shall transmit the IP packet (containing the response) from the same IP address and port on which the REGISTER request was received.

## F.4.3 General treatment for all dialogs and standalone transactions excluding the REGISTER method

### F.4.3.1 Introduction

The procedures described in subclause 5.2.6 apply with the additional procedures described in subclause F.4.3.

### F.4.3.2 Request initiated by the UE

When the P-CSCF receives, from the UE that is behind a NAT, an initial request for a dialog or a request for a standalone transaction, the P-CSCF shall:

- a) set the value of the "rport" header field parameter in the Via header field to the source port of the received IP packet that contained the request, and insert the "received" header field parameter in the Via header field containing the source IP address of the received IP packet (that contained the request), as defined in RFC-3581 [56A];
- b) if the request is a dialog-forming request that was received over UDP, bind the source IP address (i.e. the public IP address of the NAT) and associated source port number (i.e. the port number of the NAT) of the received IP packet (that contained the initial dialog-forming request) to:
  - the IP address (i.e. the private IP address of the UE) and associated port number (i.e. the private port of the UE) contained in the Contact header field of the received dialog-forming request, if the Contact header field contained an IP address and associated port number, and save the binding; or
  - the saved IP address (i.e. the private IP address of the UE) and associated port number (i.e. the private port of the UE) contained in the Contact header field of the REGISTER request, if the Contact header field of the received dialog-forming request contained a GRUU, and save the binding; and
- c) if the dialog-forming request was received over TCP connection, keep this TCP connection up during the entire duration of the dialog;

before forwarding the request, based on the topmost Route header field, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a response to the above request, the P-CSCF shall forward the response to the UE using the mechanisms described in RFC 3581 [56A]. In case UDP is used, the P-CSCF shall send the response to the IP address indicated in the "received" header field parameter and to the port indicated in the "rport" header field parameter of the Via header field of the response. If the dialog-forming request received from the UE was received over the TCP connection, the P-CSCF shall send the response to the UE over the same TCP connection over which the dialog-forming request was received. The P-CSCF shall transmit the IP packet (containing the response) from the same IP address and port on which the initial dialog-forming request was received.

For all subsequent requests belonging to the dialog, received from the UE, the P-CSCF shall insert the "received" header field parameter and set the value of the "rport" header field parameter in the Via header field as defined in RFC 3581 [56A] and forward the request as described in RFC 3261 [26]. For all subsequent responses belonging to the dialog, destined or the UE, the P-CSCF shall forward the responses using the "received" header field parameter and set the value of the "rport" header field parameter in the Via header field of the response as defined in RFC 3581 [56A].

For all subsequent requests belonging to the dialog and destined for the UE (that contains the private IP address and associated private port number in the Request-URI), the P-CSCF shall send the requests to the UE either:

- over the TCP connection that was established when the initial INVITE request was received; or
- use UDP. When sending the request using UDP, the P-CSCF shall insert the request in an IP packet, and send the IP packet to the saved IP address (i.e. the public IP address of the NAT) and associated port number (i.e. the port number of the NAT). The P-CSCF shall transmit the IP packet (containing the request) from the same IP address and port on which the REGISTER request was received.

NOTE: When inserting its SIP URI in the Record-Route header field of the dialog-forming request received from the UE, the P-CSCF can include a pointer in the user part of its SIP URI that points to the saved binding used to route the in-dialog requests to the UE. The Route header field of the in-dialog requests will contain the respective pointer in the user part of the P-CSCF's SIP URI.

### F.4.3.3 Request terminated by the UE

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction destined for the UE (it contains the private IP address and associated private port number in the Request-URI), the P-CSCF shall send the requests to the UE either:

- over the TCP connection, if available (e.g. TCP connection was established during the registration procedure); or
- use UDP. When sending the request using UDP, the P-CSCF shall insert the request in an IP packet, and send the IP packet to the saved IP address (i.e. the public IP address of the NAT) and associated port number (i.e. the port number of the NAT) that is bound to the private IP address and associated private port number indicated in the Request-URI and save during the registration procedure. The P-CSCF shall transmit the IP packet (containing the request) from the same IP address and port on which the REGISTER request was received.

For all subsequent requests belonging to the dialog that are received from the UE, the P-CSCF shall insert the "received" header field parameter and set the value of the "rport" header field parameter in the Via header field as defined in RFC 3581 [56A] and forward the request as described in RFC 3261 [26]. For all subsequent responses belonging to the dialog, destined or the UE, the P-CSCF shall forward the responses using the "received" header field parameter and set the value of the "rport" header field parameter in the Via header field of the response as defined in RFC 3581 [56A].

For all subsequent requests belonging to the dialog and destined for the UE (that contains the private IP address and associated private port number in the Request-URI), the P-CSCF shall send the requests to the UE either:

- over the TCP connection, if available; or
- use UDP. When sending the request using UDP, the P-CSCF shall insert the request in an IP packet, and send the IP packet to the saved IP address (i.e. the public IP address of the NAT) and associated port number (i.e. the port number of the NAT). The P-CSCF shall transmit the IP packet (containing the request) from the same IP address and port on which the REGISTER request was received.

NOTE: When inserting its SIP URI in the Record-Route header field in a response to the dialog-forming request received from the UE, the P-CSCF can include a pointer in the user part of its SIP URI that points to the saved binding used to route the in-dialog requests to the UE. The Route header field of the in-dialog requests will contain the respective pointer in the user part of the P-CSCF's SIP URI.

---

## F.5 NAT traversal for media flows

To allow the IMS access gateway to perform address latching, for a given UDP-based media stream, the UE shall use the same port number for sending and receiving packets.

To allow early media flows, the UE shall send keepalive messages for each UDP-based media stream as soon as an SDP offer or answer is received in order to allow the IMS access gateway to perform address latching before the call is established.

To keep NAT bindings and firewall pinholes open for the UDP-based media streams, and enable the IMS access gateway to perform address latching, the UE shall send keepalive messages for each media stream as defined in subclause K.5.2.1.

# Annex G (informative): Void

---

# Annex H (normative): IP-Connectivity Access Network specific concepts when using DOCSIS to access IM CN subsystem

## H.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is a DOCSIS cable access network.

DOCSIS (Data Over Cable Service Interface Specification) is a term referring to the ITU-T Recommendation J112 [87] Annex B standard for cable modem systems.

---

## H.2 DOCSIS aspects when connected to the IM CN subsystem

### H.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by the DOCSIS cable access network to provide packet-mode communication between the UE and the IM CN subsystem.

From the perspective of the UE, the necessary IP-CAN bearer for signalling is transparently available to the UE.

The UE is not directly involved in requests for IP-CAN bearer(s) for media flow(s). The IM CN interacts with the PCRF in the DOCSIS IP-CAN to establish IP-CAN bearer(s) for media flow(s), on behalf of the UE.

### H.2.2 Procedures at the UE

#### H.2.2.1 Activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall perform a Network Attachment procedure as defined in the CableLabs PacketCable specifications PKT-TR-ARCH-FRM [88]. When using DOCSIS, both IPv4 and IPv6 UEs may access the IM CN subsystem. The procedures for P-CSCF discovery defined in subclause 9.2.1 of this document apply.

##### H.2.2.1A Modification of IP-CAN used for SIP signalling

Not applicable.

##### H.2.2.1B Re-establishment of the IP-CAN used for SIP signalling

Not applicable.

##### H.2.2.1C P-CSCF restoration procedure

A UE supporting the P-CSCF restoration procedure uses the keep-alive procedures described in RFC 6223 [143].

If the P-CSCF fails to respond to the keep-alive request the UE shall acquire a different P-CSCF address using any of the methods described in the subclause H.2.2.1 and perform an initial registration as specified in subclause 5.1.



### H.2.2.2 Void

### H.2.2.3 Void

### H.2.2.4 Void

## H.2.2.5 Handling of the IP-CAN for media

### H.2.2.5.1 General requirements

The UE does not directly request resources for media flow(s).

#### H.2.2.5.1A Activation or modification of IP-CAN for media by the UE

Not applicable.

#### H.2.2.5.1B Activation or modification of IP-CAN for media by the network

Not applicable.

#### H.2.2.5.1C Deactivation of IP-CAN for media

Not applicable.

### H.2.2.5.2 Special requirements applying to forked responses

The UE does not directly request resources for media flow(s). As a result there are no special UE requirements applying to forked responses.

### H.2.2.5.3 Unsuccessful situations

Not applicable.

## H.2.2.6 Emergency service

If attached to network via DOCSIS access technology, the UE shall always consider being attached to its home operator's network for the purpose of emergency calls.

**NOTE:** In DOCSIS the UE is unable to receive any indication from the network, that would allow the UE to determine, whether it is currently attached to its home operator's network or to a different network, so the UE assumes itself always attached to the home operator's network when connected via DOCSIS access technology.

## H.2A Usage of SDP

### H.2A.0 General

Not applicable.

#### H.2A.1 Impact on SDP offer / answer of activation or modification of IP-CAN for media by the network

Not applicable.

#### H.2A.2 Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE

Not applicable.

## H.2A.3 Emergency service

No additional procedures defined.

---

## H.3 Application usage of SIP

### H.3.1 Procedures at the UE

#### H.3.1.1 P-Access-Network-Info header field

If the UE is aware of the access technology, the UE shall include the P-Access-Network-Info header field where indicated in subclause 5.1.

#### H.3.1.2 Availability for calls

Not applicable.

#### H.3.1.2A Availability for SMS

Void.

#### H.3.1.3 Authorization header field

When using SIP digest or SIP digest without TLS, the UE need not include an Authorization header field on sending a REGISTER request, as defined in subclause 5.1.1.2.1.

**NOTE:** In case the Authorization header field is absent, the mechanism only supports that one public user identity is associated with only one private user identity. The public user identity is set so that it is possible to derive the private user identity from the public user identity by removing SIP URI scheme and the following parts of the SIP URI if present: port number, URI parameters, and To header field parameters. Therefore, the public user identity used for registration in this case cannot be shared across multiple UEs. Deployment scenarios that require public user identities to be shared across multiple UEs that don't include an private user identity in the initial REGISTER request can be supported as follows:

- Assign each sharing UE a unique public user identity to be used for registration,
- Assign the shared public user identities to the implicit registration set of the unique registering public user identities assigned to each sharing UE.

#### H.3.1.4 SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE

Not applicable.

### H.3.2 Procedures at the P-CSCF

#### H.3.2.1 Determining network to which the originating user is attached

If access type field in the P-Access-Network-Info header field indicated DOCSIS access the P-CSCF shall assume that the initial request for a dialog or standalone transaction or an unknown method destined for a PSAP is initiated in the same country.

**NOTE 1:** If local policy does not require the insertion of P-Access-Network-Info header field in the P-CSCF even if it is missing in the received initial request, the P-CSCF can assume that the request is initiated by fixed broadband UE in the same country.

NOTE 2: If the network provided and UE provided P-Access-Network-Info header fields indicate different access types the P-CSCF ignores the information in either the network provided or the UE provided P-Access-Network-Info header field according to operator policy.

### H.3.2.2 Location information handling

Upon receipt of an initial request for a dialog or standalone transaction or an unknown method, the P-CSCF based on local policy may include a P-Access-Network-Info header field.

NOTE: The way the P-CSCF deduces that the request comes from a UE connected through DOCSIS access is implementation dependent.

## H.3.3 Procedures at the S-CSCF

### H.3.3.1 Notification of AS about registration status

Not applicable.

---

## H.4 3GPP specific encoding for SIP header field extensions

Void.

---

## H.5 Use of circuit-switched domain

There is CS domain in this access technologyVoid.

---

# Annex I (normative): Additional routing capabilities in support of transit, roaming and interconnection traffics in IM CN subsystem

## I.1 Scope

Additional routing functionality is necessary for support of:

- transit traffic as operators may use the IM CN subsystem as a transit network to provide transit functionality for their own CS networks, enterprise networks, or other network operators;
- other traffics such as roaming traffic and incoming traffic destined to CSI UEs (Combining Circuit Switched (CS) and IP Multimedia Subsystem (IMS) services) traffics; and
- traffic for the roaming architecture for voice over IMS with local breakout.

Depending on the additional routing functionalities, the required specific functions might reside in a stand-alone entity or might be collocated functional entities as appropriate for the specific scenario.

When collocated with an I-CSCF, the additional routing capabilities may be performed in advance of I-CSCF procedures as specified in subclause 5.3, or after I-CSCF procedures have failed to identify an S-CSCF supporting the user identified by the Request-URI.

When collocated with an MGCF, the generated requests can be routed to an I-CSCF or to possible targets of the routing procedures defined in subclause I.2.

The BGCF procedures specified in subclause 5.6 are a subset of the more general routing procedures provided in this annex.

NOTE: Depending on the host entity for the additional routing functions, the functionality can be accessed as:

- a) the last set of functions on the host before forwarding a request (e.g., on an MGCF, an S-CSCF or an IBCF);
- b) the first set of functions performed by the host entity when receiving a request at the host entity's entry point (e.g., on a BGCF, I-CSCF or IBCF);
- c) a specified point in the logic of the host (e.g., on the I-CSCF at failure to identify an S-CSCF for the Request-URI); or
- d) a set of functions associated with a separate entry point (e.g., at a separate entry point associated with a BGCF, I-CSCF, IBCF or separate function).

---

## I.1A General

For all SIP transactions identified, if priority is supported, as containing an authorised Resource-Priority header field, or, if such an option is supported, relating to a dialog which previously contained an authorised Resource-Priority header field. The additional routing functionality shall give priority over other transactions or dialogs. This allows special treatment of such transactions or dialogs.

NOTE 1: The special treatment can include filtering, higher priority processing, routing, call gapping. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

NOTE<sup>2</sup>: These SIP transactions are exempt from network management controls.

With the exception of 305 (Use Proxy) responses, the additional routing functionality shall not recurse on 3xx responses.

If the additional routing functionality inserts its own Record-Route header field, then the additional routing functionality may require the periodic refreshment of the session to avoid hung states. If the network element requires

the session to be refreshed, the additional routing functionality shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 3: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

Based on local policy the additional routing function shall add in requests and in responses in the P-Charging-Vector header field a "transit-ioi" header field parameter with an entry which identifies the operator network which the request or response is transitting or with a void entry.

Based on local policy the additional routing function shall delete or void in requests and in responses in the P-Charging-Vector header field any received "transit-ioi" header field parameter value.

---

## 1.2 Transit and interconnection routing procedures

The additional routing functionality, or associated functional entity, performing these additional routing procedures should analyse the destination address, and determine whether to route to another network, directly, or via the IBCF, or to the BGCF, or the I-CSCF in its own network. This analysis may use public (e.g., DNS, ENUM) and/or private database lookups, and/or locally configured data and may, based on operator policy, modify the Request-URI (e.g. to remove number prefixes, to translate local numbers to global numbers, etc).

In addition, and based upon local policy, the analysis may include the carrier identified by the "cic" tel-URI parameter of the Request-URI and other signalling information from the incoming request as part of the route determination. Examples of other signalling information are: the content of the P-Access-Network-Info header field, the value of the "cpc" tel URI parameter of the P-Asserted-Identity header field, the value of the "phone-context" Tel URI parameter of the Request-URI, the SDP content, the ICSI values in the Contact header field and the content of the P-Asserted-Service header field.

If the additional routing functionality decides that the request shall be routed via a specific entity (e.g. IBCF), it shall insert the URI of this entity in the Route header of the request.

When provided as a separate function, the network element performing these functions need not Record-Route the INVITE request.

When provided as a separate function, the network element performing these functions shall not apply the procedures of RFC 3323 [33] relating to privacy.

If overlap signalling using the multiple-INVITE method is supported as a network option, several INVITE requests with the same Call ID and same From header field (including "tag" header field parameter) can be received outside of an existing dialog. Such INVITE requests relate to the same call and the additional routing function shall route such INVITE request received during a certain period of timeto the same next hop.

When colocated with a MGCF, based on local policy for calls originated from circuit-switched networks, if the circuit-switched is a transit network the additional routing function shall add in requests in the P-Charging-Vector header field a "transit-ioi" header field parameter with an entry which identifies the PSTN network which the request was transitting or with a void entry.

NOTE 1: Only one "transit-ioi" header field parameter entry is added per transit network.

NOTE 2: The local policy can take bilateral agreements between operators into consideration.

The entity implementing the additional routing functionality shall remove the P-Served-User header field prior to forwarding the request.

---

## 1.3 Providing IMS application services in support of transit & interconnection traffics

### 1.3.1 Introduction

When the IM CN subsystem provides transit functionality to other operator networks or enterprise networks, it may also provide IMS applications services to the operator network or enterprise network.

The transit service invocation, performed by a transit function, is performed based on local configured transit invocation criteria that are provided for the specific transit scenario.

NOTE: The transit invocation criteria for invocation is intended to be per served network basis, for which transit functionality is provided, and not per subscriber basis.

Similar to the initial filter criteria for a user profile, the transit invocation criteria may have service point triggers, used to generate an ordered list of transit invocation criteria to be applied to a request, based on different information in the request, SIP method, SIP header field, and SIP body. The service invocation procedure shall support suppression/avoidance of conflicting services, multiple invocations of the same service and loopback scenarios.

## 1.3.2 Procedures

### 1.3.2.1 Treatment for dialog and standalone transactions

When the transit function receives an initial request for a dialog, or a request for a standalone transaction, and the request is received either from a functional entity within the same trust domain or contains a valid original dialog identifier (see step 3) or the dialog identifier (From, To and Call-ID header fields) relates to an existing request processed by the transit function, then prior to forwarding the request, the transit function shall:

- 1) check if an original dialog identifier that the transit function previously placed in a Route header field is present in the topmost Route header field of the incoming request.
  - If not present, the transit function shall build an ordered list of transit invocation criteria.
  - If present, the request has been sent from an AS in response to a previously sent request, an ordered list of transit invocation criteria already exists and the transit function shall not change the ordered list of transit invocation criteria.
- 2) remove its own SIP URI from the topmost Route header field;
- 3) check whether the initial request matches any unexecuted transit invocation criteria. If there is a match, then the transit function shall select the first matching unexecuted transit invocation criteria from the ordered list of transit invocation criteria and the transit function shall insert the AS URI to be contacted into the Route header field as the topmost entry followed by its own URI populated;

NOTE: Depending on the result of processing the transit invocation criteria the transit function can contact one or more AS(s) before processing the outgoing Request-URI.

- 4) if the request is not forwarded to an AS and if local policy requires the application of other additional routing capabilities, handled by entities other than the transit function, the transit function shall apply the additional routing capabilities if they are locally available or forward the request to an entity that implements the additional routing capabilities;
- 5) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header field if present, otherwise based on the Request-URI. If the destination requires interconnect functionalities (e.g. the destination address is of an IP address type other than the IP address type used in the IM CN subsystem), the transit function shall forward the request to the destination address via an IBCF in the same network;
- 6) in case of an initial request for a dialog, based on local policy record-route; and
- 7) route the request based on SIP routing procedures.

When the transit function receives a target refresh request, or a subsequent request other than target refresh request, for a dialog, prior to forwarding the request, the transit function shall:

- 1) remove its own URI from the topmost Route header field; and
- 2) forward the request based on the topmost Route header field.

With the exception of 305 (Use Proxy) responses, the transit function shall not recurse on 3xx responses.

### I.3.2.1A Handling of header fields related to charging

When the transit function receives an initial request for a dialog or a request for a standalone transaction from a functional entity that is not an AS and if the request is forwarded to an AS the transit function shall:

- store the value of the "orig-ioi" header field parameter received in the P-Charging-Vector header field if present;

NOTE 1: Any received "orig-ioi" header field parameter will be a type 2 IOI. The type 2 IOI identifies the service provider from which the request was sent.

- remove the "orig-ioi" header field parameter from the P-Charging-Vector header field, if present; and
- insert in the P-Charging-Vector header field an IOI type 3 value in an "orig-ioi" header field parameter identifying the network sending the request.

When forwarding the initial request for a dialog or the request for a standalone transaction to a functional entity that is not an AS the transit function shall:

- store the value of the "orig-ioi" header field parameter received in the P-Charging-Vector header field if present;

NOTE 2: Any received "orig-ioi" header field parameter will be a type 3 IOI. The type 3 IOI identifies the service provider from which the request was sent.

- remove the "orig-ioi" header field parameter from the P-Charging-Vector header field, if present; and
- insert in the P-Charging-Vector header field the "orig-ioi" header field parameter with the IOI type 2 value stored when the initial request for a dialog or the request for a standalone transaction was received from an entity that was not an AS.

When the transit function receives a 1xx or 2xx response to initial request for a dialog or a request for a standalone transaction from a functional entity that is not an AS and if the response is forwarded to an AS the transit function shall:

- store the values of the "orig-ioi" and the "term-ioi" header field parameter received in the P-Charging-Vector header field if present;

NOTE 3: Any received "term-ioi" header field parameter will be a type 2 IOI. The type 2 IOI identifies the service provider from which the response was sent.

- remove the "orig-ioi" and the "term-ioi" header field parameter from the P-Charging-Vector header field, if present; and
- insert in the P-Charging-Vector header field an IOI type 3 value in an "term-ioi" header field parameter identifying the network sending the response and an IOI type 3 value in an "orig-ioi" header field parameter stored when the initial request for a dialog or the request for a standalone transaction was received from an AS.

When forwarding the 1xx or 2xx response to an initial request for a dialog or a request for a standalone transaction to a functional entity that is not an AS the transit function shall:

- remove the "orig-ioi" and the "term-ioi" header field parameter from the P-Charging-Vector header field, if present; and

NOTE 4: Any received "term-ioi" and "orig-ioi" header field parameter will be a type 3 IOI. The type 3 IOI identifies the service provider from which the response was sent.

- insert in the P-Charging-Vector header field an "orig-ioi" header field parameter with the IOI type 2 value, an "term-ioi" header field parameter with the IOI type 2 value received in the 1xx or 2xx response to the initial request for a dialog or in the request for a standalone transaction from a functional entity that was not a an AS.

### I.3.2.2 Original dialog identifier for transit function

The original dialog identifier is an implementation specific token that the transit function encodes into the own transit function URI in a Route header field, prior to forwarding the request to an AS. This is possible because the transit function is the only entity that creates and consumes the value.

The token may identify the original dialog of the request, so in case an AS acting as a B2BUA changes the dialog, the transit function is able to identify the original dialog when the request returns to the transit function. In a case of a

standalone transaction, the token indicates that the request has been sent to the transit function from an AS in response to a previously sent request. The token can be encoded in different ways, such as e.g., a character string in the user-part of the transit function URI, a parameter in the transit function URI or port number in the transit function URI.

The transit function shall ensure that the value chosen is unique, in order for the transit function to recognize the value when received in a subsequent message of one or more dialogs and make the proper association between related dialogs that pass through an AS.

An original dialog identifier is sent to each AS invoked due to transit invocation criteria evaluation such that the transit function can associate requests as part of the same sequence that trigger transit invocation criteria evaluation in priority order (and not rely on SIP dialog information that may change due to B2BUA AS).

**NOTE:** If the same original dialog identifier is included in more than one request from a particular AS (based on service logic in the AS), then the transit function will continue the transit invocation criteria evaluation sequence. If the AS wants transit invocation criteria evaluation to start from the beginning for a request, then AS does not include an original dialog identifier.

---

## 1.4 Loopback routing procedures

### 1.4.1 Introduction

In order to support traffics for the roaming architecture for voice over IMS with local breakout the additional routing functionality will perform the procedures described in this subclause. An additional routing functionality performing the procedures in this subclause is always located in the visited PLMN and is referred to as Transit and Roaming Function (TRF).

The TRF performs local break out and routes the INVITE request via a specific entity e.g. IBCF or BGCF.

Loopback routing requires support in the visited network and the home network. If the visited network supports loopback routing then the P-CSCF will, based on local policy, express this support by adding a `g.3gpp.trf` feature-capability indicator value to the URI of the desired TRF.

The home network decides based on local operator policy if loopback routing shall be applied. If loopback routing is applied, the home network routes the INVITE request back to the TRF located in the visited network indicating that loopback routing is used by including the `g.3gpp.loopback` feature-capability indicator in a Feature-Caps header field.

In the loopback scenario OMR as specified in 3GPP TS 29.079 [11D] is used to determine the optimal media path between the visited network and the terminating network without passing through the home network.

### 1.4.2 TRF procedure

When the TRF receives an initial request for a dialog, the TRF shall:

- 1) store the value of the "icid-value" header field parameter received in the P-Charging-Vector header field and retain the "icid-value" header field parameter in the P-Charging-Vector header field;
- 2) store the value of the "orig-ioi" header field parameter received in the P-Charging-Vector header field, if present, and remove the "orig-ioi" header field parameter from the P-Charging-Vector header field. Insert a type 2 "orig-ioi" header field parameter into the P-Charging-Vector header field. Set the type 2 "orig-ioi" header field parameter to a value that identifies the sending network in which the TRF resides. The TRF shall not include the "term-ioi" header field parameter. Store the value of a "transit-ioi" header field parameter received in the P-Charging-Vector header field, if present, and remove the "transit-ioi" header field parameter from the P-Charging-Vector header field before forwarding the request;
- 3) if required by local policy, perform number normalization and enum translation in the same way as performed by S-CSCF in subclause 5.4.3.2 step 10);
- 4) if the P-Access-Network header field is available, determine the entity for local break out (e.g. IBCF or BGCF) using:
  - a) the location of the originating user; and
  - b) the destination address,



- then include a Route header field set to the URI associated with the determined entity in the forwarded request;
- 5) create a Record-Route header field containing the TRF own SIP URI;
  - 6) remove the "+g.3gpp.loopback" header field parameter from the Feature-Caps header field of the outgoing request; and
  - 7) route the request based on SIP routing procedures.

When the TRF receives a 1xx or 2xx response to the INVITE request above, the TRF shall:

- store the value of the "term-ioi" header field parameter and the value of the "transit-ioi" header field parameter received in the P-Charging-Vector header field and remove the "transit-ioi" header field parameter from the P-Charging-Vector header field, if present;
- remove the "orig-ioi" header field parameter and the "term-ioi" header field parameter from the P-Charging-Vector header field before forwarding the response; and

NOTE: Any received "term-ioi" header field parameter will be a type 2 IOI identifying the sending network of the response.

- insert in the P-Charging-Vector header field the "orig-ioi" header field parameter, if received in the request, and the type 1 "term-ioi" header field parameter in the response. The TRF shall set the type 1 "term-ioi" header field parameter to a value that identifies the network in which the TRF resides and the type 1 "orig-ioi" header field parameter is set to the previously received value of the type 1 "orig-ioi" header field parameter.

When the TRF receives subsequent requests or responses to subsequent requests containing the "+g.3gpp.loopback" header field parameter from the Feature-Caps header field, the TRF shall remove the "+g.3gpp.loopback" header field parameter from the Feature-Caps header field of the outgoing request or the outgoing response.

When the TRF receives responses to initial or subsequent requests from the terminating side, the TRF shall insert in the P-Charging-Vector header field, if present, the "loopback" header field parameter to the outgoing response.

When the TRF receives subsequent requests from the terminating side, the TRF shall insert in the P-Charging-Vector header field, if present, the "loopback" header field parameter to the outgoing request.

---

## 1.5 Overload control

### 1.5.1 Introduction

The additional routing functionality, or associated functional entity, performing additional routing procedures described in I.3 may support the event-based overload control mechanism.

### 1.5.2 Outgoing subscriptions to load-control event

Based on operator policy, the additional routing functionality may subscribe to the load-control event package with one or more target SIP entities. The list of target SIP entities is provisioned.

Subscription to the load-control event package is triggered by internal events (e.g. the physical device hosting the SIP entity is power-cycled) or through a management interface.

The AS shall perform subscriptions to the load-control event package to a target entity in accordance with RFC 3265 [28] and with RFC 7200 [201]. When subscribing to the load-control event, additional routing functionality shall:

- 1) Send a SUBSCRIBE request in accordance with RFC 3265 [28] and with RFC 7200 [201] to the target entity, with the following elements:
  - an Expires header field set to a network specific value;
- 2) If the target entity is located in a different network and local policy requires the application of IBCF capabilities, forward the request to an IBCF acting as an exit point.

The additional routing functionality shall automatically refresh ongoing subscriptions to the load-control event package either 600 seconds before the expiration time if the initial subscription was for greater than 1200 seconds, or when half of the time has expired if the initial subscription was for 1200 seconds or less.

The additional routing functionality can terminate a subscription according to RFC 3265 [28].

# Annex J (normative): Void

---

# Annex K (normative): Additional procedures in support of UE managed NAT traversal

## K.1 Scope

This annex describes the UE, P-CSCF, and S-CSCF procedures in support of UE managed NAT traversal. For ICE, the IBCF procedures are also described. In this scenario, both the media flows and the SIP signalling both traverse a NA(P)T device located in the customer premises domain. The term "hosted NAT" is used to address this function. This annex does not consider the case where the NAT is behind the P-CSCF as different NAT traversal procedures are necessary for this architectural scenario.

The procedures described in this subclause of this annex rely on the UE to manage the NAT traversal process. As part of the UE management process, the UE can learn whether it is behind a NAT or not, and choose whether the procedures in this annex are applied or not.

The protection of SIP messages is provided by applying either UDP encapsulation to IPSec packets in accordance with RFC 3948 [63A] and as defined in 3GPP TS 33.203 [19] or by utilizing TLS as defined in 3GPP TS 33.203 [19].

NOTE 1: This annex describes the mechanism for support of UE managed NAT traversal scenario defined in 3GPP TS 23.228 [7]. This does not preclude other mechanisms but they are out of the scope of this annex.

NOTE 2: It is recognized that outbound can be useful for capabilities beyond NAT traversal (e.g. multiple registrations) however this annex does not consider such capabilities at this time. Such capabilities can require additional information elements in the REGISTER request so that the P-CSCF and S-CSCF can distinguish whether to apply procedures as of annex F or annex K.

---

## K.2 Application usage of SIP

### K.2.1 Procedures at the UE

#### K.2.1.1 General

This subclause describes the UE SIP procedures for supporting a UE managed hosted NAT traversal approach. The description enhances the procedures specified in subclause 5.1.

#### K.2.1.2 Registration and authentication

##### K.2.1.2.1 General

The text in subclause 5.1.1.1 applies without changes.

##### K.2.1.2.1A Parameters contained in the ISIM

The text in subclause 5.1.1.1A applies without changes.

##### K.2.1.2.1B Parameters provisioned to a UE without ISIM or USIM

The text in subclause 5.1.1.1B applies without changes.

##### K.2.1.2.2 Initial registration

###### K.2.1.2.2.1 General

The procedures described in subclause 5.1.1.2.1 apply with the additional procedures described in the present subclause.

NOTE 1: In accordance with the definitions given in subclause 3.1 the IP address acquired initially by the UE in a hosted NAT scenario is the UE private IP address.

On sending a REGISTER request, the UE shall populate the header fields as indicated in subitems a) through j) of subclause 5.1.1.2 with the exceptions of subitems c) and d) which are modified as follows.

The UE shall populate:

- c) a Contact header field according to the following rules: the Contact header field shall be set to include SIP URI(s) containing the private IP address or FQDN of the UE in the hostport parameter. The UE shall also include an instance ID ("sip.instance" header field parameter) and "reg-id" header field parameter as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];
- d) a Via header field set to include the private IP address or FQDN of the UE in the sent-by field. For TCP, the response is received on the TCP connection on which the request was sent. For UDP, the UE shall include the "rport" header field parameter as defined in RFC 3581 [56A].

NOTE 2: The UE will learn its public IP address from the "received" header field parameter in the topmost Via header field in the 401 (Unauthorized) response to the unprotected REGISTER request.

NOTE 3: If the UE specifies a FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field of an unprotected REGISTER request, this FQDN will not be subject to any processing by the P-CSCF or other IMS entities.

When a 401 (Unauthorized) response to a REGISTER request is received with integrity protection the UE shall behave as described in subclause K.2.1.2.5.

When a 401 (Unauthorized) response to a REGISTER request is received and this response is received without integrity protection, the procedures described in subclause 5.1.1.2 apply with the following additions:

The UE shall compare the values in the "received" header field parameter and "rport" header field parameter with the corresponding values in the sent-by parameter in the topmost Via header field to detect if the UE is behind a NAT. If the comparison indicates that the respective values are the same, the UE concludes that it is not behind a NAT.

- if the UE is not behind a NAT the UE shall proceed with the procedures described in subclause 5.1;
- if the UE is behind a NAT the UE shall verify using the Security-Server header field that either the mechanism-name "tls" or "ipsec-3gpp" and the mode "UDP-enc-tun" is selected. If the verification succeeds the UE shall behave as described in subclause K.2.1.2.5 and store the IP address contained in the "received" header field parameter as the UE's public IP address. If the verification does not succeed the UE shall abort the registration.

On receiving the 200 (OK) response to the REGISTER request, the procedures described in subclause 5.1.1.2 apply with the following additions:

The UE shall determine the P-CSCFs ability to support the keep-alive procedures as described in RFC 5626 [92] by checking whether the "outbound" option-tag is present in the Require header field:

- if no "outbound" option-tag is present, the UE may use some other explicit indication in order to find out whether the P-CSCF supports the outbound edge proxy functionality. Such indication may be accomplished either through UE local configuration means or the UE can examine the 200 (OK) response to its REGISTER request for Path header fields, and if such are present check whether the bottommost Path header field contains the "ob" SIP URI parameter. If the UE determines that the P-CSCF supports the outbound edge proxy functionality, the UE can use the keep-alive techniques defined in subclause K.2.1.5 and RFC 5626 [92] towards the P-CSCF; or
- if an "outbound" option-tag is present, the UE shall initiate keep-alive mechanisms as defined in subclause K.2.1.5 and RFC 5626 [92] towards the P-CSCF.

NOTE 4: Presence of the "outbound" option-tag in the Require header field indicates that both the P-CSCF and S-CSCF fully support the outbound procedures. The number of subsequent outbound registrations for the same private user identity but with a different reg-id value is based on operator policy.

#### K.2.1.2.2.2 Initial registration using IMS AKA

The procedures described in subclause 5.1.1.2.2 apply with the additional procedures described in the present subclause.

On sending a REGISTER request, the UE shall populate the header fields as indicated in subclause 5.1.1.2.2 with the exceptions of the subitems which are modified as follows:

- c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the public IP address or FQDN and the protected server port value in the sent-by field. For TCP, if the REGISTER request is protected by a security association, the UE shall include the public IP address or FQDN;
- d) the Security-Client header field set to specify the security mechanisms the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the IPsec layer algorithms for integrity and confidentiality protection as defined in 3GPP TS 33.203 [19], and shall announce support for them according to the procedures defined in RFC 3329 [48]. In addition to transport mode, the UE shall support UDP encapsulated tunnel mode as per RFC 3948 [73A] and shall announce support for both modes as described in 3GPP TS 33.203 [19];

#### K.2.1.2.2.3 Initial registration using SIP digest without TLS

The procedures described in subclause 5.1.1.2.3 apply without modification.

#### K.2.1.2.2.4 Initial registration using SIP digest with TLS

The procedures described in subclause 5.1.1.2.4 apply without modification.

#### K.2.1.2.2.5 Initial registration using NASS-IMS bundled authentication

The procedures described in subclause 5.1.1.2.5 apply without modification.

#### K.2.1.2.3 Initial subscription to the registration-state event package

The procedures described in subclause 5.1.1.3 apply with the additional procedures described in subclause K.2.1.4.1.

#### K.2.1.2.4 User-initiated re-registration

##### K.2.1.2.4.1 General

The procedures described in subclause 5.1.1.4 apply with the additional procedures described in the present subclause.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as indicated in subclause 5.1.1.4.1 with the exception of subitems c) and d) which are modified as follows.

The UE shall populate:

- c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the private IP address of the UE or FQDN, its instance ID ("sip.instance" header field parameter) along with the same "reg-id" header field parameter used for the initial, successful, registration for the given P-CSCF public identity combination as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62]; and
- d) a Via header field according to the following rules:
  - For UDP, the UE shall include the public IP address or FQDN in the sent-by field. The UE shall also include the "rport" header field parameter as defined in RFC 3581 [56A]. The UE shall only use an FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT; or
  - For TCP, the UE shall include the public IP address or FQDN of the UE in the sent-by field. The UE shall only use an FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT;

When the timer F expires at the UE, the UE shall:

- 1) stop processing of all ongoing dialogs and transactions associated with that, if any (i.e. no further SIP signalling will be sent by the UE on behalf of these transactions or dialogs); and
- 2) after releasing all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2, the UE shall follow the procedures in RFC 5626 [92] to form a new flow to replace the failed one. When registering to create a new flow to replace the failed one, procedures in subclause 5.1.1.2 apply.

NOTE: These actions can also be triggered as a result of the failure of a STUN keep-alive. It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g., based on ICMP messages.

If failed registration attempts occur in the process of creating a new flow, the flow recovery procedures defined in RFC 5626 [92] shall apply.

#### K.2.1.2.4.2 IMS AKA as a security mechanism

The procedures described in subclause 5.1.1.4.2 apply without modification.

#### K.2.1.2.4.3 SIP Digest without TLS as a security mechanism

The procedures described in subclause 5.1.1.4.3 apply without modification.

#### K.2.1.2.4.4 SIP Digest with TLS as a security mechanism

The procedures described in subclause 5.1.1.4.4 apply without modification.

#### K.2.1.2.4.5 NASS-IMS bundled authentication as a security mechanism

The procedures described in subclause 5.1.1.4.5 apply without modification.

### K.2.1.2.5 Authentication

#### K.2.1.2.5.1 IMS AKA – general

The procedures of subclause 5.1.1.5.1 apply with the additional procedures described in the present subclause.

On receiving a 401 (Unauthorized) response to the REGISTER request and the response is deemed to be valid and signalling security is to be used, the UE shall behave as of subclause 5.1.1.5.1 with the exception of subitem 3) which is modified as follows.

The UE shall:

- 3) send another REGISTER request using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial registration (see subclause K.2.1.2.2), with the addition that the UE shall include an Authorization header field containing the private user identity and if the "algorithm" header field parameter is "AKAv1-MD5", the authentication challenge response shall be calculated by the UE using RES and other parameters, as described in RFC 3310 [49]. If the "algorithm" header field parameter is "MD5", the UE shall calculate SIP digest-response parameters as indicated in RFC 2617 [21] and shall build an Authorization header field based on these parameters. The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the integrity-protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

For IPsec, if the 200 (OK) response is not received before the temporary SIP level lifetime of the temporary set of security associations expires or a 403 (Forbidden) response is received, the UE shall consider the registration to have failed. The UE shall delete the temporary set of security associations it was trying to establish, and use the old set of security associations. The UE should send an unprotected REGISTER request according to the procedure specified in subclause K.2.1.2.2 if the UE considers the old set of security associations to be no longer active at the P-CSCF.

**K.2.1.2.5.2**      Void**K.2.1.2.5.3**      IMS AKA abnormal cases

The text in subclause 5.1.1.5.3 applies without changes.

**K.2.1.2.5.4**      SIP digest without TLS – general

The text in subclause 5.1.1.5.4 applies without changes.

**K.2.1.2.5.5**      SIP digest without TLS – abnormal procedures

The procedures of subclause 5.1.1.5.5 apply with the additional procedures described in the present subclause.

On receiving a 403 (Forbidden) response, the UE shall consider the registration to have failed. If performing SIP digest with TLS, the UE should send an initial REGISTER according to the procedure specified in subclause K.2.1.2.2 if the UE considers the TLS session to be no longer active at the P-CSCF.

**K.2.1.2.5.6**      SIP digest with TLS – general

The text in subclause 5.1.1.5.6 applies without changes.

**K.2.1.2.5.7**      SIP digest with TLS – abnormal procedures

The text in subclause 5.1.1.5.7 applies without changes.

**K.2.1.2.5.8**      NASS-IMS bundled authentication – general

The text in subclause 5.1.1.5.8 applies without changes.

**K.2.1.2.5.9**      NASS-IMS bundled authentication – abnormal procedures

The text in subclause 5.1.1.5.9 applies without changes.

**K.2.1.2.5.10**     Abnormal procedures for all security mechanisms

The text in subclause 5.1.1.5.10 applies without changes.

**K.2.1.2.5A**     Network initiated re-authentication

The procedures of subclause 5.1.1.5A apply with the additional procedures described in the present subclause.

On starting the re-authentication procedure sending a REGISTER request that does not contain a challenge response, the UE shall behave as of subclause 5.1.1.5A with the exception of subitem 2) which is modified as follows.

The UE shall:

- 2) start the re-authentication procedures at the appropriate time (as a result of the S-CSCF procedure described in subclause 5.4.1.6) by initiating a re-registration as described in subclause K.2.1.2.4, if required.

**K.2.1.2.5B**     Change of IPv6 address due to privacy

The text in subclause 5.1.1.5B applies without changes.

**K.2.1.2.6**      User-initiated deregistration**K.2.1.2.6.1**      General

The procedures of subclause 5.1.1.6.1 apply with the additional procedures described in the present subclause.

On sending a REGISTER request, the UE shall populate the header fields as indicated in subclause 5.1.1.6.1 with the exception of subitems c) and d) which are modified as follows.

The UE shall populate:

- c) a Contact header field set to either the value of "\*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN, its instance ID ("sip.instance" header field parameter) along with the same "reg-



id" header field parameter used for the initial, successful, registration for the given P-CSCF public identity combination as described in RFC 5626 [92];. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT;

d) a Via header field according to the following rules:

- For UDP, the UE shall include the public IP address or FQDN. The UE shall also include the "rport" header field parameter as defined in RFC 3581 [56A]. The UE shall only use an FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT; or
- For TCP, the UE shall include the public IP address or FQDN of the UE in the sent-by field. The UE shall only use an FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT;

NOTE: In case of hosted NAT traversal only the UE public IP addresses are bound to security associations or TLS session.

#### K.2.1.2.6.2 IMS AKA as a security mechanism

The text in subclause 5.1.1.6.2 applies without changes.

#### K.2.1.2.6.3 SIP digest as a security mechanism

The text in subclause 5.1.1.6.3 applies without changes.

#### K.2.1.2.6.4 SIP digest with TLS as a security mechanism

The text in subclause 5.1.1.6.4 applies without changes.

#### K.2.1.2.6.5 Initial registration using NASS-IMS bundled authentication

The text in subclause 5.1.1.6.5 applies without changes.

#### K.2.1.2.7 Network-initiated deregistration

The procedures of subclause 5.1.1.7 apply with the additional procedures described in the present subclause.

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) which were registered by this UE with:

- the state attribute set to "terminated" and the event attribute set to "rejected" or "deactivated"; or
- the state attribute set to "active" and the state attribute within the <contact> element belonging to this UE set to "terminated", and associated event attribute element to "rejected" or "deactivated";

The UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the initial registration procedure as described in subclause K.2.1.2.2. In case of a "rejected" event attribute, the UE shall release all dialogs related to those public user identities.

### K.2.1.3 Subscription and notification

The text in subclause 5.1.2 applies without changes.

#### K.2.1.4 Generic procedures applicable to all methods excluding the REGISTER method

##### K.2.1.4.1 UE-originating case

The procedures described in subclause 5.1.2A.1 apply with the additional procedures described in the present subclause.

When the UE sends any request, the requirements in subclause 5.1.2A.1 are extended by the following requirements. The UE shall include:

- a Via header field according to the following rules:

- For UDP, the UE shall include the public IP address or FQDN and the protected server port value in the sent-by field. The UE shall also include the "rport" header field parameter as defined in RFC 3581 [56A]. The UE shall only use an FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT; or
- For TCP, the UE shall include the public IP address or FQDN of the UE in the sent-by field. The UE shall only use an FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT; and
- if the request contains a Contact header field, include a Contact header field according to the following rules:
  - if this is a request for a new or existing dialog, and the UE did insert a GRUU in the Contact header field, then the UE shall also include its instance ID ("sip.instance" header field parameter), and an "ob" SIP URI parameter as described in RFC 5626 [92]; or
  - if this is a request for a new or existing dialog, and the UE did not insert a GRUU in the Contact header field, then the UE shall include the public IP address of the UE or FQDN and the protected server port value bound to the security association or TLS session in the hostport parameter along with its instance ID ("sip.instance" header field parameter), and an "ob" SIP URI parameter as described in RFC 5626 [92]. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT.

NOTE: The means to ensure that the FQDN resolves to the public IP address of the NAT are outside of the scope of this specification. One option for resolving this is local configuration.

Where a security association or TLS session exists, the UE shall discard any SIP response that is not protected by the security association or TLS session and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause K.2.1.2.

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause K.2.1.2.4.

#### K.2.1.4.2 UE-terminating case

The procedures described in subclause 5.1.2A.2 apply with the additional procedures described in the present subclause.

When the UE sends any response, the requirements in subclause 5.1.2A.2 are extended by the following requirement. If the UE did not include a GRUU in the Contact header field, then the UE shall:

- include the public IP address of the UE or FQDN and the protected server port value bound to the security association or TLS session in the hostport parameter in any Contact header field that is otherwise included. The UE shall only use a FQDN, if it is ensured that the FQDN resolves to the public IP address of the NAT.

The UE shall discard any SIP request that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause K.2.1.2.

#### K.2.1.5 Maintaining flows and detecting flow failures

STUN Binding Requests are used by the UE as a keep-alive mechanism to maintain NAT bindings for signalling flows over connectionless transport (for dialogs outside a registration as well as within a registration) as well as to determine whether a flow (as described in RFC 5626 [92]) is still valid (e.g. a NAT reboot could cause the transport parameters to change). As such, the UE acts as a STUN client and shall follow the requirements defined by RFC 5389 [100]. Further, when using UDP encapsulated IPsec, the keep-alive capabilities defined within should not be used.

CRLF as defined in RFC 5626 [92] is used by the UE as a keep-alive mechanism to maintain NAT bindings for signalling flows over connection oriented transports (for dialogs outside a registration as well as within a registration) as well as to determine whether a flow (as described in RFC 5626 [92]) is still valid (e.g. a NAT reboot could cause the transport parameters to change). As such, the UE shall follow the requirements defined by RFC 5626 [92].

If the UE determines that the flow to a given P-CSCF is no longer valid (the UE does not receive a STUN reply (or CRLF) or the reply indicates a new public IP Address) the UE shall consider the flow and any associated security associations invalid and perform the initial registration procedures defined in subclause K.2.1.2.2.

When a NAT is not present, it may not be desirable to send keep-alive requests (i.e. given battery considerations for wireless UEs). As such, if a UE can reliably determine that a NAT is not present (i.e. by comparing the "received" and

"rport" header field parameters in the Via header field in the response to the initial un-protected REGISTER request with the locally assigned IP Address and Port) then the UE may not perform the keep-alive procedures.

## K.2.1.6 Emergency services

### K.2.1.6.1 General

In addition to the procedures in subclause 5.1.6.1, the following additional procedures apply. When receiving and sending requests unprotected, the UE shall transmit and receive all SIP messages using the same IP port.

### K.2.1.6.2 Initial emergency registration

When a UE performs an initial emergency registration the UE shall perform the actions as specified in subclause K.2.1.2.2. The remaining procedures described in subclause 5.1.6.2 apply without modification.

#### K.2.1.6.2A New initial emergency registration

The text in subclause 5.1.6.2A applies without changes.

### K.2.1.5A.3 Initial subscription to the registration-state event package

The text in subclause 5.1.6.3 applies without changes.

### K.2.1.6.4 User-initiated emergency reregistration

The UE shall perform user-initiated emergency reregistration as specified in subclause K.2.1.2.4. The remaining procedures described in subclause 5.1.6.4 apply without modification.

### K.2.1.6.5 Authentication

The UE shall perform the authentication procedures as specified in subclause K.2.1.2.5. The remaining procedures described in subclause 5.1.6.5 apply without modification.

### K.2.1.6.6 User-initiated emergency deregistration

The text in subclause 5.1.6.6 applies without changes.

### K.2.1.6.7 Network-initiated emergency deregistration

The text in subclause 5.1.6.7 applies without changes.

### K.2.1.6.8 Emergency session setup

#### K.2.1.6.8.1 General

The text in subclause 5.1.6.8.1 applies without changes.

#### K.2.1.6.8.2 Emergency session set-up in case of no registration

The text in subclause 5.1.6.8.2 applies without changes.

#### K.2.1.6.8.3 Emergency session set-up with an emergency registration

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause K.2.1.4, subclause 5.1.3, and subclause 5.1.4. The remaining procedures described in subclause 5.1.6.8.3 apply without modification.

#### K.2.1.6.8.4 Emergency session set-up within a non-emergency registration

The UE shall apply the procedures as specified in subclause K.2.1.4, subclause 5.1.3, and subclause 5.1.4. The remaining procedures described in subclause 5.1.6.8.4 apply without modification.

### K.2.1.6.9 Emergency session release

The text in subclause 5.1.6.9 applies without changes.

## K.2.2 Procedures at the P-CSCF

### K.2.2.1 Introduction

This subclause describes the SIP procedures for supporting hosted NAT scenarios.

The description enhances the procedures specified in subclause 5.2.

### K.2.2.2 Registration

#### K.2.2.2.1 General

The procedures described in subclause 5.2.2.1 apply without changes.

#### K.2.2.2.2 IMS AKA as a security mechanism

The procedures described in subclause 5.2.2.2 apply with the additional procedures described in the present subclause.

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall behave as in subclause 5.2.2.2 with the exception of subitems 2) and 3) which are modified as follows.

- 2) in case the REGISTER request was received without protection, then:
  - a) check the existence of the Security-Client header field. If the Security-Client header field is not present and signalling security is used, then the P-CSCF shall return a suitable 4xx response. If the Security-Client header field is present the P-CSCF shall:
    - in case the UE indicated support for "UDP-enc-tun" then remove and store it; or
    - in case the UE does not indicate support for "UDP-enc-tun" then:
      - if the host portion of the sent-by field in the topmost Via header field contains an IP address that differs from the source address of the IP packet, silently drop the REGISTER request;
    - otherwise continue with procedures as of subclause 5.2.2.2;

NOTE 2: If the UE does not indicate support for "UDP-enc-tun" and the P-CSCF detects that the UE is located behind a NAT device, then the P-CSCF can just drop the REGISTER request to avoid unnecessary signalling traffic.

- 3) in case the REGISTER request was received integrity protected, then the P-CSCF shall:
  - a) check the security association which protected the request. If IPsec is used and the security association is a temporary one the P-CSCF shall:
    - in case the hostport parameter in the Contact address is in the form of a FQDN, ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address bound to the security association;
    - in case the P-CSCF has detected earlier that the UE is located behind a NAT and IPsec is being used, retrieve port\_Uenc from the encapsulating UDP header of the packet received and complete configuration of the temporary set of security associations by configuring port\_Uenc in each of the temporary security associations;
    - check whether the request contains a Security-Verify header field in addition to a Security-Client header field. If there are no such header fields, then the P-CSCF shall return a suitable 4xx response. If there are such header fields, then the P-CSCF shall compare the content of the Security-Verify header field with the content of the Security-Server header field sent earlier and the content of the Security-Client header field with the content of the Security-Client header field received in the challenged REGISTER request. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header field;

When the P-CSCF receives a 401 (Unauthorized) response to an unprotected REGISTER request and the P-CSCF previously determined that the UE is behind a NAT and the UE indicated support for "UDP-enc-tun" IPsec mode, the P-CSCF shall:

- 1) delete any temporary set of security associations established towards the UE;
- 2) for IPsec, remove the "ck" and "ik" WWW-Authenticate header field parameters contained in the 401 (Unauthorized) response and bind the values to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the "ck" and "ik" header field parameters have been removed;
- 3) insert a Security-Server header field in the response, containing the P-CSCF security list and the parameters needed. The P-CSCF shall support the setup of two pairs of security associations, as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed of the IPsec security association setup is specified in annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the IPsec layer algorithms for integrity protection and for encryption as defined in 3GPP TS 33.203 [19]. The P-CSCF shall indicate "UDP-enc-tun" as the only IPsec mode.
- 4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. The P-CSCF shall select UDP encapsulated tunnel mode and shall leave the value for port-Uenc unspecified in each of the temporary security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and
- 5) send the 401 (Unauthorized) response unprotected to the UE using the mechanisms described in RFC 3261 [26] and RFC 3581 [56A], i.e. the P-CSCF shall send the response to the IP address indicated in the "received" header field parameter and, in case UDP is used, to the port indicated in the "rport" header field parameter (if present) of the Via header field associated with the UE. In case TCP is used as transport protocol, the P-CSCF shall use the port on which the REGISTER request was received as client port for sending the response back to the UE.

When the P-CSCF receives a 401 (Unauthorized) response to a protected REGISTER request and the P-CSCF previously determined that the UE is behind a NAT and that REGISTER request was protected by an old set of security associations that use UDP encapsulated tunnel mode, the P-CSCF shall:

- 1) delete any temporary set of security associations established towards the UE;
- 2) remove the "ck" and "ik" WWW-Authenticate header field parameters contained in the 401 (Unauthorized) response and bind the values to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the "ck" and "ik" header field parameters have been removed;
- 3) insert a Security-Server header field in the response, containing the P-CSCF security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the IPsec layer algorithms for integrity protection and encryption as defined in 3GPP TS 33.203 [19]. The P-CSCF shall indicate "UDP-enc-tun" as the IPsec mode;
- 4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. The P-CSCF shall select UDP encapsulated tunnel mode and shall specify the same port\_Uenc that was used in the old set of security associations. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and
- 5) send the 401 (Unauthorized) response to the UE using the old set of security associations and using the rules for sending responses as described in RFC 3261 [26] and RFC 3581 [56A], i.e. the P-CSCF shall send the response to the IP address indicated in the "received" header field parameter and to the port indicated in the "rport" header field parameter (if present) of the Via header field associated with the UE. Otherwise, when the P-CSCF receives a 401 (Unauthorized) response to an unprotected REGISTER request and this response does not contain a "received" header field parameter and "rport" header field parameter or when the P-CSCF receives a 401 (Unauthorized) response to a protected REGISTER request and that REGISTER request was protected by an old set of security associations that do not use UDP encapsulated tunnel mode, the P-CSCF shall proceed as described in subclause 5.2.2.2 of the main body of this specification.

#### K.2.2.2.3 SIP digest without TLS as a security mechanism

The text in subclause 5.2.2.3 applies without changes.

#### K.2.2.2.4 SIP digest with TLS as a security mechanism

The procedures described in subclause 5.2.2.4 apply without changes.

#### K.2.2.2.5 NASS-IMS bundled authentication as a security mechanism

The text in subclause 5.2.2.5 applies without changes.

### K.2.2.3 General treatment for all dialogs and standalone transactions excluding the REGISTER method

#### K.2.2.3.1 Requests initiated by the UE

##### K.2.2.3.1.1 General for all requests

The procedures described in subclause 5.2.6.3.1 apply with the additional procedures described in the present subclause.

When the P-CSCF receives from the UE an initial request for a dialog or a request for a standalone transaction, the requirements are extended by the following requirements.

Before forwarding the request, based on the topmost Route header field, in accordance with the procedures of RFC 3261 [26], the P-CSCF shall ensure that all signalling during the lifetime of the dialogue is sent over the same IMS flow set as the dialogue initiating request.

**NOTE:** The suggested way to ensure all signalling is sent over the same IMS flow set is to form an IMS flow token in the same way that a P-CSCF would form this for the Path header field and insert this IMS flow token in the user portion of the URI used in the record route header field value.

##### K.2.2.3.1.2 General for all responses

The procedures in subclause 5.2.6.3.2 apply without changes.

##### K.2.2.3.1.2A Abnormal cases

The text in subclause 5.2.6.3.2A applies without changes.

##### K.2.2.3.1.3 Initial request for a dialog

The text in subclause 5.2.6.3.3 applies without changes.

##### K.2.2.3.1.4 Responses to an initial request for a dialog

The text in subclause 5.2.6.3.4 applies without changes.

##### K.2.2.3.1.5 Target refresh request for a dialog

The text in subclause 5.2.6.3.5 applies without changes.

##### K.2.2.3.1.6 Responses to a target refresh request for a dialog

The text in subclause 5.2.6.3.6 applies without changes.

##### K.2.2.3.1.7 Request for a standalone transaction

The text in subclause 5.2.6.3.7 applies without changes.

##### K.2.2.3.1.8 Responses to a request for a standalone transaction

The text in subclause 5.2.6.3.8 applies without changes.

##### K.2.2.3.1.9 Subsequent request other than a target refresh request

The text in subclause 5.2.6.3.9 applies without changes.

K.2.2.3.1.10 Responses to a subsequent request other than a target refresh request

Void

K.2.2.3.1.11 Request for an unknown method that does not relate to an existing dialog

The text in subclause 5.2.6.3.11 applies without changes.

K.2.2.3.1.12 Responses to a request for an unknown method that does not relate to an existing dialog

Void

K.2.2.3.2 Requests terminated by the UE

K.2.2.3.2.1 General for all requests

Void

K.2.2.3.2.2 General for all responses

Void

K.2.2.3.2.3 Initial request for a dialog

The procedures described in subclause 5.2.6.4.3 apply with the additional procedures described in the present subclause.

When the P-CSCF receives, destined for the UE, a request, the requirements are extended by the following requirements. The P-CSCF shall:

- forward the request to the terminating UE over the appropriate flow within the denoted IMS flow set.

K.2.2.3.2.4 Responses to an initial request for a dialog

The text in subclause 5.2.6.4.4 applies without changes.

K.2.2.3.2.5 Target refresh request for a dialog

The procedures described in subclause 5.2.6.4.5 apply with the additional procedures described in the present subclause.

When the P-CSCF receives, destined for the UE, a request, the requirements are extended by the following requirements. The P-CSCF shall:

- forward the request to the terminating UE over the appropriate flow within the denoted IMS flow set.

K.2.2.3.2.6 Responses to a target refresh request for a dialog

The text in subclause 5.2.6.4.6 applies without changes.

K.2.2.3.2.7 Request for a standalone transaction

The procedures described in subclause 5.2.6.4.7 apply with the additional procedures described in the present subclause.

When the P-CSCF receives, destined for the UE, a request, the requirements are extended by the following requirements. The P-CSCF shall:

- forward the request to the terminating UE over the appropriate flow within the denoted IMS flow set.

K.2.2.3.2.8 Responses to a request for a standalone transaction

The text in subclause 5.2.6.4.8 applies without changes.

K.2.2.3.2.9 Subsequent request other than a target refresh request

The procedures described in subclause 5.2.6.4.9 apply with the additional procedures described in the present subclause.

When the P-CSCF receives, destined for the UE, a request, the requirements are extended by the following requirements. The P-CSCF shall:

- forward the request to the terminating UE over the appropriate flow within the denoted IMS flow set.

#### K.2.2.3.2.10 Responses to a subsequent request other than a target refresh request

The text in subclause 5.2.6.4.10 applies without changes.

#### K.2.2.3.2.11 Request for an unknown method that does not relate to an existing dialog

Void

#### K.2.2.3.2.12 Responses to a request for an unknown method that does not relate to an existing dialog

Void

### K.2.2.4 Void

### K.2.2.5 Emergency services

#### K.2.2.5.1 General

The procedures described in subclause 5.2.10.1 apply without changes.

#### K.2.2.5.2 General treatment for all dialogs and standalone transactions excluding the REGISTER method – from an unregistered user

The procedures described in subclause 5.2.10.2 apply with the additional procedures described in the present subclause.

When the P-CSCF receives from the UE an initial request for a dialog or a request for a standalone transaction, the requirements are extended by the following requirements.

Before forwarding the request, based on the topmost Route header field, in accordance with the procedures of RFC 3261 [26], the P-CSCF shall ensure that all signalling during the lifetime of the dialogue is sent over the same IMS flow set as the dialogue initiating request.

- NOTE: The suggested way to ensure all signalling is sent over the same IMS flow set is to form an IMS flow token in the same way that a P-CSCF would form this for the Path header field and insert this IMS flow token in the user portion of the URI used in the Record-Route header field value.

#### K.2.2.5.3 General treatment for all dialogs and standalone transactions excluding the REGISTER method after emergency registration

The procedures described in subclause 5.2.10.3 apply with the additional procedures described in the present subclause.

When the P-CSCF receives from the UE an initial request for a dialog, or a standalone transaction, or an unknown method, the following requirements:

- 1) include in the Request-URI an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69], if necessary, and execute the procedure described in step 4, 5, 6, and 7, in subclause 5.2.6.3.3, subclause 5.2.6.3.7, subclause 5.2.6.3.11, subclause 5.2.7.2 and subclause K.2.2.3.1, as appropriate. An additional sub-service type can be added if information on the type of emergency service is known. The entry in the Request-URI that the P-CSCF includes may either be:
  - as received from the UE in the Request-URI in accordance with RFC 5031 [69]; or
  - as deduced from the Request-URI received from the UE.

#### K.2.2.5.4 General treatment for all dialogs and standalone transactions excluding the REGISTER method – non-emergency registration

The procedures described in subclause 5.2.10.4 apply with the additional procedures described in the present subclause.



When the P-CSCF receives from the UE an initial request for a dialog, or a standalone transaction, or an unknown method, the following requirements are extended:

- 1) include in the Request-URI an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69], if necessary, and execute the procedure described in step 3, 4, 5, 6, and 7, in subclause 5.2.6.3.3, subclause 5.2.6.3.7, subclause 5.2.6.3.11 subclause 5.2.7.2 and subclause K.2.2.3.1, as appropriate. An additional sub-service type can be added if information on the type of emergency service is known. The entry in the Request-URI that the P-CSCF includes may either be:
  - as received from the UE in the Request-URI in accordance with RFC 5031 [69]; or
  - as deduced from the Request-URI received from the UE; and

#### K.2.2.5.5 Abnormal cases

The text in subclause 5.2.10.5 applies without changes.

#### K.2.3 Void

#### K.2.4 Void

---

### K.3 Application usage of SDP

#### K.3.1 UE usage of SDP

The procedures as of subclause 6.1 apply.

#### K.3.2 P-CSCF usage of SDP

The procedures as of subclause 6.2 apply.

---

#### K.4 Void

### K.5 Application usage of ICE

#### K.5.1 Introduction

The following subclauses describe the usage of the Interactive Connectivity Establishment (ICE) procedures as documented in RFC 5245 [99]

#### K.5.2 UE usage of ICE

##### K.5.2.1 General

NAT bindings also need to be kept alive for media. RFC 5245 [99] provides requirements for STUN based keepalive mechanisms. UEs that do not implement the ICE procedures as defined in RFC 5245 [99] should implement the keepalive procedures defined in RFC 5245 [99]. In the case where keepalives are required and the other end does not support ICE (such that STUN cannot be used for a keepalive) or the UE can not discover STUN or TURN servers to gather candidates, the UE shall send an empty (no payload) RTP packet with a payload type of 20 as a keepalive as long as the other end has not negotiated the use of this value. If this value has already been negotiated, then some other unused static payload type from table 5 of RFC 3551 [55A] shall be used. When sending an empty RTP packet, the UE shall continue using the sequence number (SSRC) and timestamp as the negotiated RTP stream.

##### K.5.2.2 Call initiation – UE-origination case

The UE should support the agent requirements for ICE as defined by RFC 5245 [99] when sending the initial INVITE request. RFC 5245 [99] provides procedures for:

- 1) Gathering candidate addresses for RTP and RTCP prior to sending the INVITE;
- 2) Encoding the candidate addresses in the SDP that is included with the INVITE;
- 3) Acting as a STUN server to receive binding requests from the remote client when it does connectivity checks;
- 4) Performing connectivity checks on received candidate addresses for RTP and RTCP;
- 5) Determining and possibly selecting a better active address based on the requirements in RFC 5245 [99];
- 6) Subsequent offer/answer exchanges; and
- 7) Sending media.

When supporting the ICE procedures, the UE shall also support the STUN agent requirements as described in RFC 5389 [100] in order to gather STUN addresses, the TURN client requirements as described in RFC 5766 [101] in order to gather TURN Server addresses and the STUN Server requirements defined in RFC 5245 [99] as well as the requirements for STUN Servers defined in RFC 5389 [100] for responding to connectivity checks.

RFC 5245 [99] provides an algorithm for determining the priority of a particular candidate. The following additional requirements are provided to the UE:

- 1) The type preference assigned for each type of candidate from least to highest should be: Relayed Transport Address, STUN address, local address; and
- 2) If the UE has a dual IPv4/IPv6 stack, IPv6 addresses may be assigned a higher local preference than IPv4 addresses based on the operator's policy.

RFC 5245 [99] provides guidance on choosing the in-use candidate and recommends that a UE choose relayed candidates as the in-use address. The following additional requirements are provided to the UE:

- 1) If a TURN server is available, the Relayed Transport Address should be used as the initial active transport address (i.e. as advertised in the m/c lines of the SDP); and
- 2) If a TURN server is not available, an address obtained via STUN should be used as the initial active transport address.

Regardless of whether the UE supports the above procedures, the UE shall, upon receipt of an SDP answer with candidate addresses, perform connectivity checks on the candidate addresses as described in RFC 5245 [99]. In order to perform connectivity checks, the UE shall act as a STUN client as defined in RFC 5389 [100]. Further, the UE shall also follow the procedures in RFC 5245 [99] when sending media.

### K.5.2.3 Call termination – UE-termination case

The UE should support agent requirements for ICE as defined by RFC 5245 [99] when receiving an initial INVITE request. RFC 5245 [99] provides procedures for:

- 1) Gathering candidate addresses for RTP and RTCP prior to sending the answer as described in RFC 5245 [99];
- 2) Encoding the candidate addresses in the SDP answer as described in RFC 5245 [99];
- 3) Acting as a STUN server to receive binding requests from the remote client when it does connectivity checks;
- 4) Performing connectivity checks on received candidate addresses for RTP and RTCP;
- 5) Determining and possibly selecting a better active address based on the requirements in RFC 5245 [99];
- 6) Subsequent offer/answer exchanges; and
- 7) Sending media.

When supporting the ICE procedures, the UE shall also support the STUN agent requirements as described in RFC 5389 [100] in order to gather STUN addresses, the TURN client requirements as described in RFC 5766 [101] in order to gather TURN Server addresses and the STUN Server requirements defined in RFC 5245 [99] as well as the requirements for STUN Servers defined in RFC 5389 [100] for responding to connectivity checks.

RFC 5245 [99] provides an algorithm for determining the priority of a given candidate. The additional requirements for the UE:

- 1) The priority of candidate addresses from least to highest should be: Relayed Transport Address, STUN address, local address; and
- 2) If the UE has a dual IPv4/IPv6 stack, IPv6 addresses MAY be placed at a higher priority than IPV4 addresses based on the operator's policy.

RFC 5245 [99] provides guidance on choosing the in-use candidate and recommends that a UE choose relayed candidates as the in-use address. The following additional requirements are provided to the UE:

- 1) If a TURN server is available, the Relayed Transport Address should be used as the initial active transport address (i.e. as advertised in the m/c lines of the SDP); and
- 2) If a TURN server is not available, an address obtained via STUN should be used as the initial active transport address.

Regardless of whether the UE supports the above procedures, the UE shall, upon receipt of an SDP offer with candidate addresses, perform connectivity checks on the candidate addresses as described in RFC 5245 [99]. In order to perform connectivity checks, the UE shall act as a STUN client as defined in RFC 5389 [100]. Further, the UE shall also follow the procedures in RFC 5245 [99] when sending media.

When receiving an SDP offer which does not indicate support for ICE, the UE aborts the ICE procedures and reverts to RFC 3264 [27B] offer/answer procedures; per RFC 5245 [99]. However, if the terminating UE is behind a NA(P)T device this may result in the inability to pass media for the session as the terminating UE will respond with its locally assigned IP address which is unreachable. In order to ensure successful media exchange, the terminating UE shall provide either a STUN derived IP address and port or a TURN provided IP address and port in the m/c lines of the SDP answer. If the provided address and port is a TURN address and port, the policy charging and control framework will be unable to establish proper filter criteria as the address is that of the TURN server and not that of the UE or NAT in front of the UE; see RFC 5245 [99] subclause B.3 for further details. To rectify this issue, the terminating UE shall also include a candidate attribute as described in RFC 5245 [99] identifying the server reflexive IP address and port (i.e. the IP address and port on the public side of the NAT) used when a TURN provided address and port is provided in the m/c line of the SDP answer.

### K.5.3 P-CSCF support of ICE

The P-CSCF procedures to support ICE as specified in RFC 5245 [99] are defined in subclause 6.7.2.7.

### K.5.4 Void

---

# Annex L (normative): IP-Connectivity Access Network specific concepts when using EPS to access IM CN subsystem

## L.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is Evolved Packet System (EPS). The EPS IP-CAN has an EPS core network which can be supported by an E-UTRAN radio access network.

---

## L.2 EPS aspects when connected to the IM CN subsystem via E-UTRAN

### L.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by EPS to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the UE on the use of these packet-mode services are specified in this clause. Requirements for the P-GW in support of this communication are specified in 3GPP TS 29.061 [11], and 3GPP TS 29.212 [13B].

When using the EPS, each IP-CAN bearer is provided by an EPS bearer.

### L.2.2 Procedures at the UE

#### L.2.2.1 EPS bearer context activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

- a) if not attached for EPS services yet, perform a EPS attach procedure as specified in 3GPP TS 24.301 [8J];
- b) ensure that a EPS bearer context used for SIP signalling according to the APN and P-GW selection criteria described in 3GPP TS 23.401 [7B], is available. This EPS bearer context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the EPS bearer context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

NOTE 3: The default EPS bearer context can also be used for SIP signalling as well as any other EPS bearer context.

When the EPS bearer context establishment procedure for the SIP signalling is initiated by the UE:

- I. if a default EPS bearer context is not available with the selected P-GW, the UE shall indicate to the network in the PDN CONNECTIVITY REQUEST that the request is for SIP signalling. If the request is authorized, the network establishes a bearer with the appropriate QCI as described in 3GPP TS 24.301 [8J]. The UE may also use this EPS bearer context for DNS and DHCP signalling;
- II. if the default EPS bearer context is available with the selected P-GW, and is to be used for SIP signalling no additional steps are needed;
- III. if the default EPS bearer context is available with the selected P-GW and an EPS bearer for SIP signalling with the correct QCI and TFT is to be established, the UE shall indicate to the network, by setting the IM CN Subsystem Signalling Flag in the Protocol Configuration Options information element in the BEARER RESOURCE ALLOCATION REQUEST message, that the request is for SIP signalling. If the request is authorized, the network either establishes a new dedicated bearer or modifies an existing bearer with the appropriate QCI and TFT as described in 3GPP TS 24.301 [8J]. The general QoS negotiation mechanism is described in 3GPP TS 24.301 [8J].

NOTE 2: An EPS bearer with a QCI value other than the one for signalling can carry both IM CN subsystem signalling and media, in case the media does not need to be authorized by Policy and Charging control mechanisms as defined in 3GPP TS 29.212 [13B] and the media stream is not mandated by the P-CSCF to be carried in a separate EPS bearer.

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.

II. Transfer P-CSCF address(es) within the EPS bearer context activation procedure.

The UE shall indicate the request for a P-CSCF address to the network within the Protocol Configuration Options information element of the PDN CONNECTIVITY REQUEST message or BEARER RESOURCE ALLOCATION REQUEST message.

If the network provides the UE with a list of P-CSCF IPv4 or IPv6 addresses in the ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message or ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST message, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options information element as the P-CSCF address with the highest priority.

III. The UE selects a P-CSCF from the list (see 3GPP TS 31.103 [15B]) stored in the ISIM.

IV. The UE selects a P-CSCF from the list in IMS management object.

The UE shall use method IV to select a P-CSCF, if

- a P-CSCF is to be discovered in the home network;
- the UE is roaming; and
- the IMS management object contains the P-CSCF list.

The UE shall use method III to select the P-CSCF, if:

- a P-CSCF is to be discovered in the home network;
- the UE is roaming;
- either the UE does not contain the IMS management object, or the UE contains the IMS management object but the IMS management object does not contain the P-CSCF list; and
- the ISIM residing in the UICC supports the P-CSCF list.

The UE can freely select method I or II for P-CSCF discovery, if:

- the UE is in the home network; or
- the UE is roaming and the P-CSCF is to be discovered in the visited network.

In case method I is selected and several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3361 [35A] when using IPv4 or RFC 3319 [41] when using IPv6. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

NOTE 3: The UE decides whether the P-CSCF is to be discovered in the serving network or in the home network based on local configuration, e.g. whether the application on the UE is permitted to use local breakout.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

If the UE is configured to use Option II above and detects that all P-CSCFs known by the UE have been used when the UE selects a different P-CSCF as a result of:

- receiving 305 (Use Proxy) to the REGISTER request;
- receiving 504 (Server Time-out); or
- expiration of the timer F at the UE,

then if there are more than one PDN connection that UE is connected to and unless the IP-CAN bearer is in use by other applications, the UE shall:

- 1) release IP-CAN bearer that is used only for the transport of SIP signalling and that are not used for other non-IMS applications, but shall not release emergency IP-CAN bearers; and
- 2) unless the UE decides the service is no longer needed,
  - a) perform a new P-CSCF discovery procedure as described in subclause 9.2.1; and
  - b) perform the procedures for initial registration as described in subclause 5.1.1.2.

When using IPv4, the UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or by the Protocol Configuration Options information element when activating a EPS bearer context according to 3GPP TS 24.301 [8J].

When using IPv6, the UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options information element when activating a EPS bearer context according to 3GPP TS 24.301 [8J].

The encoding of the request and response for IPv4 or IPv6 address(es) for DNS server(s) and list of P-CSCF address(es) within the Protocol Configuration Options information element is described in 3GPP TS 24.301 [8J].

### L.2.2.1A Modification of a EPS bearer context used for SIP signalling

The EPS bearer context shall not be modified from being used exclusively for SIP signalling to a general purpose EPS bearer. After the establishment of an EPS bearer context used for SIP signalling, the UE shall not set the IM CN Subsystem Signalling Flag in the Protocol Configuration Options information element of any subsequent BEARER RESOURCE MODIFICATION REQUEST message for that APN. The UE shall ignore the IM CN Subsystem Signalling Flag if received from the network in the Protocol Configuration Options information element.

After the establishment of a EPS bearer context used for SIP signalling, the UE shall not indicate the request for a P-CSCF address to the network within the Protocol Configuration Options information element of any subsequent BEARER RESOURCE MODIFICATION REQUEST message for that APN. The UE shall ignore P-CSCF address(es) if received from the network in the Protocol Configuration Options information element.

### L.2.2.1B Re-establishment of the EPS bearer context for SIP signalling

If the UE registered a public user identity with an IP address allocated for the APN of the EPS bearer context used for SIP signalling, the EPS bearer context used for SIP signalling is deactivated as result of signalling from the network and:

- i) if the UE is required to perform an initial registration according to subclause L.3.1.2;
- ii) if the signalling from the network results in requiring the UE to initiate activation of the PDN connection of the EPS bearer context used for SIP signalling; or
- iii) if the UE needs to continue having a public user identity registered with an IP address allocated for the APN;

the UE shall:

- A) if the non-access stratum is performing the UE requested PDN connectivity procedure and the EPS bearer context activation procedure(s) for the APN triggered as result of the signalling from the network, wait until the UE requested PDN connectivity procedure and the EPS bearer context activation procedure(s) for the APN finish; and
- B) perform the procedures in subclause L.2.2.1, bullets a), b) and c).

If none of the bullets i), ii) and iii) of this subclause evaluate to true, or the procedures in bullet B) of this subclause were unable to ensure that the EPS bearer context used for SIP signalling is available or were unable to acquire any P-CSCF address(es):

- 1) if the SIP signalling was carried over a dedicated EPS bearer context, the UE shall release all resources established as a result of SIP signalling by sending to the network either:
  - a) a BEARER RESOURCE MODIFICATION REQUEST message, if there are EPS bearer contexts to this PDN that are not related SIP sessions; or
  - b) a PDN DISCONNECT REQUEST message if all the EPS bearer contexts to this PDN are related to SIP sessions.

NOTE: If the SIP signalling was carried over the default EPS bearer context, all the resources established as a result of SIP signalling are released without any explicit NAS signalling.

If the default EPS bearer context of the PDN connection of the EPS bearer context used for SIP signalling was deactivated at the start of this subclause, and the procedures in bullet B) of this subclause ensured that the EPS bearer context used for SIP signalling is available and acquired the P-CSCF address(es), the UE shall perform a new initial registration according to subclause 5.1.1.2.

### L.2.2.1C P-CSCF restoration procedure

A UE supporting the P-CSCF restoration procedure performs one of the following procedures:

- A if the UE used method II for P-CSCF discovery and if the UE receives one or more P-CSCF address(es) in the Protocol Configuration Options information element of an Modify EPS Bearer Context Request message the one or more P-CSCF address(es) do not include the address of the currently used P-CSCF, then the UE shall acquire a different P-CSCF address from the one or more P-CSCF address(es) in the Modify EPS Bearer Context Request message. If more than one P-CSCF address with the same container identifier (i.e. "P-CSCF IPv6 Address" or "P-CSCF IPv4 Address") are included, then the UE shall assume that the more than one P-CSCF addresses with the same container identifier are prioritised with the first P-CSCF address with the same container identifier within the Protocol Configuration Options information element as the P-CSCF address with the highest priority;
- B if the UE uses RFC 6223 [143] as part of P-CSCF restoration procedures, and if the P-CSCF fails to respond to a keep-alive request, then the UE shall acquire a different P-CSCF address using one of the methods I, III and IV for P-CSCF discovery described in the subclause L.2.2.1.

When a different P-CSCF address is acquired the UE shall perform an initial registration as specified in subclause 5.1.

### L.2.2.2 Session management procedures

The existing procedures for session management as described in 3GPP TS 24.301 [8J] shall apply while the UE is connected to the IM CN subsystem.

### L.2.2.3 Mobility management procedures

The existing procedures for mobility management as described in 3GPP TS 24.301 [8J] shall apply while the UE is connected to the IM CN subsystem.

### L.2.2.4 Cell selection and lack of coverage

The existing mechanisms and criteria for cell selection as described in 3GPP TS 36.304 [19B] shall apply while the UE is connected to the IM CN subsystem.

## L.2.2.5 EPS bearer contexts for media

### L.2.2.5.1 General requirements

NOTE 1: In EPS, the UE cannot control whether media streams belonging to different SIP sessions are established on the same EPS bearer context or not. During establishment of a session, the UE establishes data streams(s) for media related to the session. Such data stream(s) can result in activation of additional EPS bearer context(s). Either the UE or the network can request for resource allocations for media, but the establishment and modification of the EPS bearer is controlled by the network as described in 3GPP TS 24.301 [8J].

NOTE 2: When the UE wishes to allocate bandwidth for RTP and RTCP, the UE uses the rules as those outlined in 3GPP TS 29.213 [13C].

If the resource allocation is initiated by the UE, the UE starts reserving resources whenever it has sufficient information about the media streams, and used codecs available as specified in 3GPP TS 24.301 [8J].

NOTE 3: If the resource reservation requests are initiated by the EPS IP CAN, then the bearer establishment is initiated by the network after the P-CSCF has authorised the respective IP flows and provided the QoS requirements over the Rx interface to the PCRF as described in 3GPP TS 29.214 [13D].

#### L.2.2.5.1A Activation or modification of EPS bearer contexts for media by the UE

If the UE is configured not to initiate resource allocation for media according to 3GPP TS 24.167 [8G], then the UE shall refrain from requesting additional EPS bearer context(s) for media until the UE considers that the network did not initiate resource allocation for the media.

#### L.2.2.5.1B Activation or modification of EPS bearer contexts for media by the network

If the UE receives an activation request from the network for a EPS bearer context which is associated with the EPS bearer context used for signalling, the UE shall, based on the information contained in the Traffic Flow Template information element, correlate the media EPS bearer context with a currently ongoing SIP session establishment or SIP session modification.

If the UE receives a modification request from the network for a EPS bearer context that is used for one or more media streams in an ongoing SIP session, the UE shall:

- 1) modify the related EPS bearer context in accordance with the request received from the network.

#### L.2.2.5.1C Deactivation of EPS bearer context for media

When a data stream for media related to a session is released, if the EPS bearer resource transporting the data stream is no longer needed and allocation of the EPS bearer resource was requested by the UE, then the UE releases the EPS bearer resource.

NOTE: The EPS bearer resource can be needed e.g. for other data streams of a session or for other applications in the UE.

### L.2.2.5.2 Special requirements applying to forked responses

NOTE 1: The procedures in this subclause only apply when the UE requests activation and modification of media bearers. In the case where the network activates and modifies the media bearers the network takes care of the handling of media bearers in the case of forking.

Since the UE does not know that forking has occurred until a second, provisional response arrives, the UE requests resource allocation as required by the initial response received. If a subsequent provisional response is received, different alternative actions may be performed depending on the requirements in the SDP answer:

- 1) the bearer requirements of the subsequent SDP can be accommodated by the existing resources requested. The UE performs no further resource requests.
- 2) the subsequent SDP introduces different QoS requirements or additional IP flows. The UE requests further resource allocation according to subclause L.2.2.5.1.



- 3) the subsequent SDP introduces one or more additional IP flows. The UE requests further resource allocation according to subclause L.2.2.5.1.

NOTE 2: When several forked responses are received, the resources requested by the UE are the "logical OR" of the resources indicated in the multiple responses to avoid allocation of unnecessary resources. The UE does not request more resources than proposed in the original INVITE request.

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall release all the unneeded IP-CAN resources. Therefore, upon the reception of the first final 200 (OK) response for the INVITE request (in addition to the procedures defined in RFC 3261 [26] subclause 13.2.2.4), the UE shall:

- 1) in case resources were established or modified as a consequence of the INVITE request and forked provisional responses that are not related to the accepted 200 (OK) response, send release request to release the unneeded resources.

### L.2.2.5.3 Unsuccessful situations

One of the Rx and Gx interface related error codes can be received by the UE in either the PDN CONNECTIVITY REJECT message, the BEARER RESOURCE MODIFICATION REJECT message, or the BEARER RESOURCE ALLOCATION REJECT message. If the UE receives a Rx and Gx interface related error code, the UE shall either handle the resource reservation failure as described in subclause 6.1.1 or retransmit the message up to three times. The Rx and Gx interface related error codes are further specified in 3GPP TS 29.214 [13D] and 3GPP TS 29.212 [13B].

### L.2.2.6 Emergency service

Emergency bearers are defined for use in emergency calls in EPS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these EPS bearer contexts for both signalling and media for emergency calls made using the IM CN subsystem.

Some jurisdictions allow emergency calls to be made when the UE does not contain an ISIM or USIM, or where the credentials are not accepted. Additionally where the UE is in state EMM-REGISTERED.LIMITED-SERVICE and EMM-REGISTERED.PLMN-SEARCH, a normal ATTACH has been attempted and it can also be assumed that a registration in the IM CN subsystem will also fail. In such cases, the procedures for emergency calls without registration apply, as defined in subclause 5.1.6.8.2.

When activating a EPS bearer context to perform emergency registration, the UE shall request a PDN connection for emergency bearer services as described in 3GPP TS 24.301 [8J]. The procedures for EPS bearer context activation and P-CSCF discovery, as described in subclause L.2.2.1 of this specification apply accordingly.

In order to find out whether the UE is attached to the home PLMN or to the visited PLMN, the UE shall compare the MCC and MNC values derived from its IMSI with the MCC and MNC of the PLMN the UE is attached to. If the MCC and MNC of the PLMN the UE is attached to do not match with the MCC and MNC derived from the IMSI, then for the purpose of emergency calls in the IM CN subsystem the UE shall consider to be attached to a VPLMN.

NOTE 1: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 [4C] will be considered as a visited network.

The type of emergency service for an emergency number is derived from the settings of the emergency service category value (bits 1 to 5 of the emergency service category value as specified in subclause 10.5.4.33 of 3GPP TS 24.008 [8]). Table L.2.2.6.1 below specifies mappings between a type of emergency service and an emergency service URN. The UE shall use the mapping to match an emergency service URN and a type of emergency service. If a dialled number is an emergency number but does not map to a type of emergency service the service URN shall be "urn:service:sos".

**Table L.2.2.6.1: Mapping between type of emergency service and emergency service URN**

| Type of emergency service | Emergency service URN     |
|---------------------------|---------------------------|
| Police                    | urn:service:sos.police    |
| Ambulance                 | urn:service:sos.ambulance |
| Fire Brigade              | urn:service:sos.fire      |
| Marine Guard              | urn:service:sos.marine    |
| Mountain Rescue           | urn:service:sos.mountain  |

NOTE 2: It is not possible for a UE to indicate more than one type of emergency service in an emergency service URN.

If the IP-CAN did not provide a local emergency number that matches the dialled number (see subclause 5.1.6.1) and multiple types of emergency service can be derived for a dialled number from the information configured on the USIM then:

- if the UE is in the HPLMN, the UE shall map any one of these types of emergency service to an emergency service URN as specified in table L.2.2.6.1; and
- if the UE is in the VPLMN, the UE shall select "urn:service:sos".

If the IP-CAN provided a local emergency number that matches the dialled number (see subclause 5.1.6.1), and:

- if the UE can derive one or more types of emergency service from the information received from the IP-CAN for the dialled number and the UE cannot derive types of emergency service from the information configured on the USIM for the dialled number; or
- if the UE is able to derive identical types of emergency service from both the information received from the IP-CAN for the dialled number and from the information configured on the USIM for the dialled number,

then the UE shall map any one of these emergency service types to an emergency service URN as specified in table L.2.2.6.1.

NOTE 3: How the UE resolves clashes where an emergency number is associated with one or more different types of emergency service configured in the USIM and in information received from the access network, is implementation dependent.

Upon reception of a 380 (Alternative Service) response to an INVITE request as defined in subclause 5.1.2A.1.1 and subclause 5.1.3.1, if:

- the 380 (Alternate Service) response contains a Contact header field;
- the value of the Contact header field is a service URN; and
- the service URN has a top-level service type of "sos";

then the UE determines that "emergency service information is included" as described 3GPP TS 23.167 [4B], else the UE determines that "emergency service information" as described 3GPP TS 23.167 [4B] is not included.

If the "emergency service information is included" as described 3GPP TS 23.167 [4B]:

- 1) if the URN in the Contact header field matches an emergency service URN in table L.2.2.6.1, then the type of emergency service is the value corresponding to the matching entry in table L.2.2.6.1; and
- 2) if the URN in the Contact header field does not match any emergency service URN in table L.2.2.6.1, then the type of emergency service is not identified.

NOTE 4: In bullet 2), the URN in the Contact header field either contains "no emergency subservice type" as described in 3GPP TS 23.167 [4B] triggering an emergency call, or contains an "emergency subservice type that does not map into an emergency service category for the CS domain" as described in 3GPP TS 23.167 [4B] triggering a normal call when the dialled number is available or triggering an emergency call when the dialled number is not available.

---

## L.2A Usage of SDP

### L.2A.0 General

NOTE 1: When:

- establishing a session which is not an emergency session; or
- modifying a session which is not an emergency session;

and if the IMSVoPS indicator is received in the EPS network feature support information element (see 3GPP TS 24.301 [8J]) and no persistent EPS bearer context exists at the UE, the UE constructs SDP based on the restrictions indicated in the IMSVoPS indicator. Regardless whether the IMSVoPS indicator indicating voice is supported or not, m-lines can be set to "audio" and exclude voice codecs from the SDP answer or SDP offer. When a persistent EPS bearer context exists, m-lines can be set to "audio" and include voice codecs in the SDP answer or SDP offer.

NOTE 2: When the UE is accessing the IM CN subsystem via E-UTRAN, the appropriate specification for access domain selection is 3GPP TS 23.221 [6].

## L.2A.1 Impact on SDP offer / answer of activation or modification of EPS bearer context for media by the network

If, due to the activation of EPS bearer context from the network the related SDP media description needs to be changed, the UE shall update the related SDP information by sending a new SDP offer within a SIP request, which is sent over the existing SIP dialog,

If the UE receives a modification request from the network for a EPS bearer context that is used for one or more media streams in an ongoing SIP session, the UE shall:

- 1) if, due to the modification of the EPS bearer context, the related SDP media description need to be changed, update the related SDP information by sending a new SDP offer within a SIP request, that is sent over the existing SIP dialog, and respond to the EPS bearer context modification request.

NOTE: The UE can decide to indicate additional media streams as well as additional or different codecs in the SDP offer than those used in the already ongoing session.

## L.2A.2 Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE

If the UE receives an SDP offer where the SDP offer includes all media streams for which the originating side indicated its local preconditions as met, if the precondition mechanism is supported by the terminating UE and the IP-CAN performs network-initiated resource reservation for the terminating UE and the available resources are not sufficient for the received offer, the terminating UE shall indicate its local preconditions and provide the SDP answer to the originating side without waiting for resource reservation.

NOTE: If the resource reservation is controlled by the EPS IP-CAN, the resource reservation request is initiated by the network after the P-CSCF has authorised the respective IP flows and provided the QoS requirements over the Rx interface to the PCRF as described in 3GPP TS 29.214 [13D].

## L.2A.3 Emergency service

NOTE: When establishing an emergency session or when modifying an emergency session, the IMSVoPS indicator does not influence handling of SDP offer and SDP answer.

---

# L.3 Application usage of SIP

## L.3.1 Procedures at the UE

### L.3.1.1 P-Access-Network-Info header field

The UE shall always include the P-Access-Network-Info header field where indicated in subclause 5.1.

### L.3.1.2 Availability for calls

This subclause documents the minimal requirements for being available for voice communication services when using EPS.

A UE shall perform an initial registration as specified in subclause 5.1.1.2 using an EPS bearer context for SIP signalling (see annex L.2.2.1), if all the following conditions are met:

- 1) if the UE is operating in one of the following modes of operation (see 3GPP TS 24.301 [8J]):
  - a) PS mode 1;
  - b) CS/PS mode 1 and the UE is attached for EPS-Services only;
- 2) if the UE is capable of receiving any (but not necessarily all) of the media types which the CS domain supports, such that the media type can also be used when accessing the IM CN subsystem using the current IP-CAN;
- 3) if the media type of item 2 is an "audio" media type, and the UE supports codecs suitable for (conversational) speech;
- 4) if the UE determines that its contact has not been bound to a public user identity using the IP-CAN, such that the contact is expected to be used for the delivery of incoming requests in the IM CN subsystem relating to the media of item 2 and item 3;
- 5) if the IMSVoPS indicator, provided by the lower layers (see 3GPP TS 24.301 [8J]), indicates voice is supported;
- 6) if the procedures to perform the initial registration are enabled (see 3GPP TS 24.305 [8T]); and
- 7) if the EPS bearer context used for SIP signalling is:
  - a) available; or
  - b) not available, and the UE:
    - i. is allowed to send a PDN CONNECTIVITY REQUEST message to establish an EPS bearer context that is needed for performing the initial registration; or
    - ii. is allowed to send a BEARER RESOURCE ALLOCATION REQUEST message, wishes to establish an EPS bearer with the correct QCI and TFT for performing the initial registration, and a default EPS bearer context for the APN exists.

NOTE 1: 3GPP TS 24.301 [8J] specifies conditions that prevent the UE from sending a PDN CONNECTIVITY REQUEST message or a BEARER RESOURCE ALLOCATION REQUEST message.

NOTE 2: Regardless of any of the above conditions, a UE might attempt to register with the IM CN subsystem at any time.

EXAMPLE: As an example of the note, a UE configured to preferably attempt to use the EPS to access IM CN subsystem can perform an initial registration as specified in subclause 5.1.1.2, if the conditions in items 2, 3, 4, 5, 6 and 7 in this subclause, evaluate to true.

The UE indicates to the non-access stratum the status of being available for voice over PS when:

- I) the UE is capable of receiving any (but not necessarily all) of the media types which the CS domain supports, such that the media type can also be used when accessing the IM CN subsystem using the current IP-CAN;
- II) if the media type of item I is an "audio" media type, and the UE supports codecs suitable for (conversational) speech; and
- III) the UE determines a contact has been bound to a public user identity using the IP-CAN, such that this contact is expected to be used for the delivery of incoming requests in the IM CN subsystem relating to such media.

The UE indicates to the non-access stratum the status of being not available for voice over PS when:

- I) in response to receiving the IMSVoPS indicator indicating voice is supported, the UE:
  - initiated an initial registration as specified in subclause 5.1.1.2, received a final response to the REGISTER request sent, but the conditions for indicating the status of being available for voice over PS are not met; or
  - did not initiate an initial registration as specified in subclause 5.1.1.2 and, these conditions for indicating the status of being available for voice over PS are not met; or

II) the conditions for indicating the status of being available for voice over PS are no longer met.

### L.3.1.2A Availability for SMS

The UE determines whether the UE is able to use SMS using IMS when the UE:

- I) is capable of using the MIME type "application/vnd.3gpp.sms" (see 3GPP TS 24.341 [8L]), such that the MIME type can also be used when accessing the IM CN subsystem using the current IP-CAN;
- II) supports the role of an SM-over-IP sender (see 3GPP TS 24.341 [8L]);
- IIA) determines the EPS bearer context used for SIP signalling exists; and
- III) determines a contact has been bound to a public user identity using the IP-CAN, such that this contact is expected to be used for the delivery of incoming requests in the IM CN subsystem relating to such media.

When above criteria are not matched UE determines SMS using IMS is unavailable.

### L.3.1.3 Authorization header field

Void.

### L.3.1.4 SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE

Upon receiving an INVITE request not including the "precondition" option-tag in the Supported header field and not including the "precondition" option-tag in the Require header field, and the IP-CAN performs network-initiated resource reservation for the UE, the UE:

- 1) if the INVITE request contains an SDP offer and the local resources required at the terminating UE for the received SDP offer are not available:
  - a) shall not alert the user; and
  - b) shall send 183 (Session Progress) response to the INVITE request without waiting for resource reservation and without alerting the user. If the INVITE request includes a Supported header field indicating support of reliable provisional responses, the UE shall send the 183 (Session Progress) response reliably. In the 183 (Session Progress) response, the UE shall include an SDP answer; and
- 2) if the INVITE request does not contain an SDP offer and the INVITE request includes a Supported header field indicating support of reliable provisional responses:
  - a) shall generate an SDP offer;
  - b) if the local resources required at the terminating UE for the generated SDP offer are not available:
    - A) shall not alert the user; and
    - B) shall reliably send 183 (Session Progress) response to the INVITE request without waiting for resource reservation and without alerting the user. In the 183 (Session Progress) response, the UE shall include the generated SDP offer.

Upon successful reservation of local resources, if the precondition mechanism is not used by the terminating UE, the UE can send 180 (Ringing) response to the INVITE request and can alert the user.

## L.3.2 Procedures at the P-CSCF

### L.3.2.1 Determining network to which the originating user is attached

If the P-CSCF is configured to handle emergency requests, in order to determine from which network the request was originated the P-CSCF shall check the MCC and MNC fields received in the P-Access-Network-Info header field.

NOTE: The above check can be against more than one MNC code stored in the P-CSCF.

### L.3.2.2 Location information handling

Void.

### L.3.2.3 Prohibited usage of PDN connection for emergency bearer services

If the P-CSCF detects that a UE uses a PDN connection for emergency bearer services for a non-emergency REGISTER request, the P-CSCF shall reject that request by a 403 (Forbidden) response.

NOTE: By assigning specific IP address ranges for a PDN connection for emergency bearer services and configuring those ranges in P-CSCF, the P-CSCF can detect based on the registered Contact address if UE uses an emergency PDN connection for initial registration.

## L.3.3 Procedures at the S-CSCF

### L.3.3.1 Notification of AS about registration status

Not applicable.

---

## L.4 3GPP specific encoding for SIP header field extensions

### L.4.1 Void

---

## L.5 Use of circuit-switched domain

There is no CS domain in this access technology.

---

# Annex M (normative): IP-Connectivity Access Network specific concepts when using cdma2000<sup>®</sup> packet data subsystem to access IM CN subsystem

## M.1 Scope

This annex defines IP-CAN specific requirements for call control protocol for use in the IM CN subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is the cdma2000<sup>®</sup> packet data subsystem. It also defines procedures for invoking CS domain services.

---

## M.2 cdma2000<sup>®</sup> packet data subsystem aspects when connected to the IM CN subsystem

### M.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by the cdma2000<sup>®</sup> packet data subsystem to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the UE on the use of these packet-mode services are specified in this subclause. Requirements for the IP-CAN bearer control point (i.e. the point where the UE has attached itself to the cdma2000<sup>®</sup> packet data subsystem) support of this communication are specified in 3GPP2 X.S0011-E [127].

### M.2.2 Procedures at the UE

#### M.2.2.1 Establishment of IP-CAN bearer and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

- a) establish a connection with the cdma2000<sup>®</sup> wireless IP network specified in 3GPP2 X.S0011-E [127]. Upon establishment a connection with the cdma2000<sup>®</sup> wireless IP network, the UE can have an IPv4 address only, an IPv6 address only, or both IPv4 and IPv6 addresses simultaneously;
- b) ensure that an IP-CAN bearer used for SIP signalling is available. This IP-CAN bearer shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the last deregistration.

The UE shall choose one of the following options when performing establishment of this IP-CAN bearer:

I. A dedicated IP-CAN bearer for SIP signalling:

The UE shall indicate to the IP-CAN bearer control point that this is an IP-CAN bearer intended to carry IM CN subsystem-related signalling only. The UE may also use this IP-CAN bearer for DNS and DHCP access.

II. A general-purpose IP-CAN bearer:

The UE may decide to use a general-purpose IP-CAN bearer to carry IM CN subsystem-related signalling. The UE may carry both signalling and media on the general-purpose IP-CAN bearer;

- c) discover a P-CSCF.

The methods for P-CSCF discovery are:

I. Use DHCP mechanism

II Retrieve the list of P-CSCF address(es) stored in the IMC

### III Obtain the list of P-CSCF address(es) from the IMS management object

The UE can freely select method I, II, or III for P-CSCF discovery. If DHCP is used, the following procedures apply:

Upon establishing an IP-CAN bearer, the UE may use the Dynamic Host Configuration Protocol (DHCP) specified in RFC 2131 [40A] or Dynamic Host Configuration Protocol for IPv6 (DHCPv6) specified in RFC 3315 [40] to discover the P-CSCF.

Prior to accessing the DHCP server, the UE will have obtained an IP address via means other than DHCP and DHCPv6, see 3GPP2 X.S0011-E [127].

If the UE uses DHCP for P-CSCF discovery and the UE is unaware of the address of the DHCP server, the UE shall send the DHCPINFORM using the limited broadcast IP address (i.e., 255.255.255.255) and UDP port 67. If the UE knows the IP address of the DHCP server, the UE shall send the DHCPINFORM to the DHCP server's unicast IP address and UDP port 67. The DHCP server shall send the DHCPACK on the IP address specified in the Client IP Address field of the DHCPINFORM. The DHCP server may include, in the DHCPACK, the SIP Server DHCP Option specified in RFC 3361 [35A], which carries either a list of IPv4 address(es) of the P-CSCF(s) or a list of DNS fully qualified domain name(s) that can be mapped to one or more P-CSCF(s). If the UE uses DHCPv6 for P-CSCF discovery and the UE is unaware of the address of the DHCP Server, the UE shall send an Information Request using the IPv6 multicast address FF02::1:2 and the UDP port 547. If the UE knows the IP address of the DHCPv6 server, the UE shall send the Information Request message to the DHCPv6 server's IP address and UDP port 547. In the Information Request, the UE may request either one or both the SIP Servers Domain Name List option and the SIP Servers IPv6 Address List option specified in RFC 3319 [41]. The DHCP server shall send the Reply to the IP address specified in the Information Request. The DHCP server may include in the Reply either one or both the SIP Servers Domain Name List option and the SIP Servers IPv6 Address List option, as requested by the UE.

In case several P-CSCF's IP addresses or domain names are provided to the UE, the UE shall perform P-CSCF selection according to RFC 3361 [35A] or RFC 3319 [41]. The UE shall perform the procedure for the resolution of domain name according to RFC 3263 [27A].

#### M.2.2.1 Modification of IP-CAN used for SIP signalling

Not applicable.

#### M.2.2.1B Re-establishment of the IP-CAN used for SIP signalling

Not applicable.

#### M.2.2.1C P-CSCF restoration procedure

A UE supporting the P-CSCF restoration procedure uses the keep-alive procedures described in RFC 6223 [143].

If the P-CSCF fails to respond to the keep-alive request the UE shall acquire a different P-CSCF address using any of the methods described in the subclause M.2.2.1 and perform an initial registration as specified in subclause 5.1.

#### M.2.2.2 Void

#### M.2.2.3 IP-CAN bearer control point support of DHCP based P-CSCF discovery

The IP-CAN bearer control point, or Home Agent in case of Mobile IP with reverse tunneling, may forward the packet to one or more local DHCP servers, or relay the packet to a specific DHCP server. The IP-CAN bearer control point, or Home Agent in case of Mobile IP with reverse tunnelling, shall not forward the DHCPINFORM (or Information-Request) to any UE.

NOTE 1: For forwarding the DHCPINFORM or Information-Request, the IP-CAN bearer control point, or Home Agent in case of Mobile IP with reverse tunnelling, does not change the destination IP address of the packet.



NOTE 2: For relaying the DHCPINFORM or Information-Request, the IP-CAN bearer control point, or Home Agent in case of Mobile IP with reverse tunnelling inserts a DHCP server's IP address in the destination IP address field of the packet.

## M.2.2.4 Void

## M.2.2.5 Handling of the IP-CAN for media

### M.2.2.5.1 General requirements

Not applicable.

#### M.2.2.5.1A Activation or modification of IP-CAN for media by the UE

Not applicable.

#### M.2.2.5.1B Activation or modification of IP-CAN for media by the network

Not applicable.

#### M.2.2.5.1C Deactivation of IP-CAN for media

Not applicable.

### M.2.2.5.2 Special requirements applying to forked responses

Not applicable.

### M.2.2.5.3 Unsuccessful situations

Not applicable.

## M.2.2.6 Emergency service

When establishing an HRPD session to perform emergency registration, the UE shall follow the procedures defined in 3GPP2 X.S0060 [86B].

To determine whether the HRPD UE is attached to the home network or to the visited network, the UE shall compare the Carrier ID values obtained per 3GPP2 X.S0060 [86B]. If the Carrier ID of the network the UE is attached to does not match with the provisioned Carrier ID, then for the purpose of emergency calls in the IM CN subsystem the UE shall consider to be attached to a visited network.

NOTE: For 3GPP2-1X and 3GPP2-UMB, no IP-CAN specific support is provided in the current release. No carrier identification is provided for 3GPP2-1X or 3GPP2-UMB in the P-Access-Network-Info header field, and thus there is no IMS specific procedure for identifying that the UE is in the home network.

## M.2A Usage of SDP

### M.2A.0 General

Not applicable.

#### M.2A.1 Impact on SDP offer / answer of activation or modification of IP-CAN for media by the network

Not applicable.

## M.2A.2 Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE

Not applicable.

## M.2A.3 Emergency service

No additional procedures defined.

---

# M.3 Application usage of SIP

## M.3.1 Procedures at the UE

### M.3.1.1 P-Access-Network-Info header field

The UE shall always include the P-Access-Network-Info header field where indicated in subclause 5.1.

### M.3.1.2 Availability for calls

Not applicable.

### M.3.1.2AAvailability for SMS

Void.

### M.3.1.3 Authorization header field

When using SIP digest or SIP digest without TLS, the UE need not include an Authorization header field on sending a REGISTER request, as defined in subclause 5.1.1.2.1.

**NOTE:** In case the Authorization header field is absent, the mechanism only supports that one public user identity is associated with only one private user identity. The public user identity is set so that it is possible to derive the private user identity from the public user identity by removing SIP URI scheme and the following parts of the SIP URI if present: port number, URI parameters, and To header field parameters. Therefore, the public user identity used for registration in this case cannot be shared across multiple UEs. Deployment scenarios that require public user identities to be shared across multiple UEs that don't include an private user identity in the initial REGISTER request can be supported as follows:

- Assign each sharing UE a unique public user identity to be used for registration,
- Assign the shared public user identities to the implicit registration set of the unique registering public user identities assigned to each sharing UE.

### M.3.1.4 SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE

Not applicable.

## M.3.2 Procedures at the P-CSCF

### M.3.2.1 Determining network to which the originating user is attached

For an HRPD UE, after the initial request for a dialog or standalone transaction or an unknown method is received the P-CSCF shall check the Carrier ID field received in the P-Access-Network-Info header field to determine from which network the request was originated.

NOTE: For 3GPP2-1X and 3GPP2-UMB, no IP-CAN specific support is provided in the current release. No carrier identification is provided for 3GPP2-1X or 3GPP2-UMB in the P-Access-Network-Info header field, and thus there is no IMS specific procedure for identifying that the UE is in the home network.

### M.3.2.2 Location information handling

Void

## M.3.3 Procedures at the S-CSCF

### M.3.3.1 Notification of AS about registration status

The procedures described in subclause 5.4.1.7 apply with the additional procedures described in the present subclause:

- 1) in case the received REGISTER request contained a Timestamp header field, the S-CSCF shall insert a Timestamp header field with the value of the Timestamp header field from the received REGISTER request.

---

## M.4 3GPP specific encoding for SIP header field extensions

### M.4.1 Void

---

## M.5 Use of circuit switched domain

When an emergency call is to be set up over the CS domain, the UE shall attempt it according to the procedures described in 3GPP2 C.S0005-D [85].

---

# Annex N (Normative): Functions to support overlap signalling

## N.1 Scope

This annex defines the procedures performed by network entities within the IM CN subsystem to support overlap signalling.

The support of overlap signalling within the IM CN subsystem is optional, and is depended on the network policy.

---

## N.2 Digit collection function

### N.2.1 General

The digit collection function is invoked if an entity requires additional digits for a decision where to route a INVITE request.

NOTE 1: The digit collection function is only applicable for the in-dialog method of overlap signalling. Further information about digit collection is provided in subclause 4.9.3.3.

The digit collection function may interact with a routing database, to reach this decision. The digit collection function shall be performed by an entity acting as a B2BUA. The digit collection function requires the ability to recognise incomplete numbers. The digit collection function may be implemented in different network nodes depending on the operator's deployment strategy (e.g. AS, IBCF).

NOTE 2: An HSS does not support the recognition of incomplete numbers. A routing database being queried by ENUM also does not support the recognition of incomplete numbers.

NOTE 3: A private routing database to support the recognition of incomplete numbers e.g. for transit calls or ported numbers can be used.

### N.2.2 Collection of digits

#### N.2.2.1 Initial INVITE request

Upon receiving an initial INVITE request carrying an SDP offer, the digit collection function shall:

- 1) if the request contains enough digits to forward the request, forward the request towards its destination;
- 2) if the digit collection function chooses to collect additional digits in INFO requests, in order to forward the request, and the sender of the INVITE request has indicated support of reliable responses, store the received digits and send a reliable 183 (Session Progress) provisional response in order to establish an early dialog with the sender of the INVITE request. The response shall not contain an SDP answer; or
- 3) if it is determined that the en-bloc will not be able to forward the request even if additional digits are received,, send a 404 (Not Found) response.

Upon receiving an initial INVITE request without an SDP offer, the digit collection function shall:

- 1) if the request contains enough digits to forward the request, forward the request towards its destination; or
- 2) send a 404 (Not Found) response.

NOTE 1: If the initial INVITE request does not contain an SDP offer, a reliable 18x provisional response generated by the en-bloc conversion function would have to contain an SDP offer. In this case digit collection needs to be performed by the originating SIP entity (e.g. MGCF).

When the digit collection function sends the reliable 183 (Session Progress) provisional response, in order to establish an early dialog with the sender of the INVITE request, the digit collection function shall start a digit collection timer. If

the timer expires, the digit collection function shall terminate the call setup by sending a 484 (Address Incomplete) response towards the sender of the INVITE request.

NOTE 2: The digit collection timer is similar to the protection timer used in PSTN/ISDN. The timer value range is between 5 and 15 seconds, and the default value is 10 seconds.

### N.2.2.2 Collection of additional digits

Upon receiving an INFO request carrying additional digits, and if an early dialog towards the destination of the initial INVITE request for the call does not exist, the digit collection function shall:

- 1) send a 200 (OK) response to the INFO request;
- 2) add the received digits to the previously stored digits for the call;
- 3) restart the digit collection timer; and
- 4) check if enough digits have been received in order to forward the initial INVITE request.

When enough digits for the call have been received in order to forward the initial INVITE request, the digit collection function shall add all stored digits to the request URI and forward the request towards its destination and stop the digit collection timer.

Upon receiving an INFO request carrying additional digits, and the initial INVITE request has been forwarded towards its destination, but an early dialog towards the destination of the initial INVITE request for the call does not exist, the digit collection function shall:

- 1) send a 200 (OK) response to the INFO request; and
- 2) add the received digits to the previously stored, but yet not forwarded, digits for the call;

When the digit collection function receives a provisional response from the destination of the initial INVITE request, and the digit collection function has received additional digits in INFO requests, the digit collection shall generate and send an INFO request towards the destination of the initial INVITE request. The Request-URI shall contain all digits which have been received and stored since the initial INVITE request was forwarded.

Upon receiving an INFO request carrying additional digits, and if an early dialog towards the destination of the initial INVITE request for the call does exist, the digit collection function shall forward the INFO request on the early dialog towards the destination of the initial SIP INVITE request.

Upon receiving an INFO request carrying additional digits, and if a 180 (Ringing) or a 200 (OK) response to the initial INVITE request for the call has been received, or the digit collection function has received some other indication that enough digits have been forwarded in order for the INVITE request to reach the terminating SIP user, the digit collection function shall, based on operator policy:

- 1) send a 200 (OK) response to the INFO request and not forward the INFO request; or
- 2) forward the INFO request on the early dialog towards the destination of the initial SIP INVITE request.

### N.2.2.3 Handling of 404 (Not Found) / 484 (Address Incomplete) responses

Upon receiving a 404/484 response to the initial INVITE request, the digit collection function shall acknowledge the response and shall start the digit collection timer. The digit collection function shall not forward the response towards the sender of the INVITE request.

NOTE: If the digit collection function has received a 404/484 response, it will send a new initial INVITE request when it has received additional digits as described above, in order to establish an early dialog towards the destination of the INVITE request. The digit collection timer will re-start if an INFO request with additional digits is received. At timer expiry, the digit collection function will terminate the call as described above

## N.2.3 Forwarding of SIP messages by the digit collection function

Apart from 404/484 responses to the initial INVITE request, and INFO requests carrying additional digits received after a 180 (Ringing) or a 200 (OK) response to the initial INVITE request has been received, the digit collection function

shall forward all SIP messages. When forwarding SIP messages, the digit collection function shall modify the SIP messages to comply with SIP procedures on both call legs as specified below:

- 1) The digit collection function will receive a "tag" To header field parameter value from the receiver of the initial INVITE request, which is different from the "tag" To header field parameter value that the digit collection function inserted in the 183 (Session Progress) response that it sent when it received the initial INVITE request. The digit collection function shall modify the "tag" header field parameter value accordingly when forwarding mid-dialog SIP messages.
- 2) The digit collection function will return a Contact header field in the initial 183 (Session Progress) provisional response to the originating side, which contains a SIP-URI of the digit collection function. The contact information is used in the Request-URI of subsequent mid-dialog SIP requests sent by the originating side, until the digit collection function has received, and forwarded to the originating side, a 183 (Session Progress) provisional response from the destination of the INVITE request. If the Request-URI of the received mid-dialog SIP request contains the SIP-URI of the digit collection function, and the digit collection function forwards the request, the digit collection function shall modify the Request-URI before forwarding the SIP request.
- 3) The digit collection function will return the Record-Route header fields, which it received in the initial INVITE request, in the initial 183 (Session Progress) provisional response to the originating side. The information is used in the Route header fields of subsequent mid-dialog SIP requests sent by the originating side, until the digit collection function has received, and forwarded to the originating side, a 183 (Session Progress) provisional response from the destination of the INVITE request. If the Route header fields of the received mid-dialog SIP request are based on the Record-Route headers fields which the digit collection function returned in the initial 183 (Session Progress) provisional response, and the digit collection function forwards the request, the digit collection function shall modify the Route header fields before forwarding the SIP request.

---

## N.3 En-bloc conversion function

### N.3.1 General

The en-bloc conversion function may be performed in an entity acting as B2BUA. The en-bloc conversion function may be implemented in different network nodes depending on the operator's deployment strategy (e.g. AS, IBCF).

If the initial INVITE request is to be forwarded towards a network, or towards a network entity, that does not support overlap signalling, the en-bloc conversion function shall determine the end of address signalling.

The following methods can be used to determine the end of the address signalling:

- 1) the maximum number of digits used in a national numbering plan has been received;
- 2) number analysis, e.g. using a provisioned dial plan, is used to determine that the complete number of digits has been received; or
- 3) an inter digit timer expires, and the minimum number of digits required for routing the call have been received. The timer is started when the initial INVITE request is received, and re-started every time new digit(s) are received.

**NOTE:** The inter digit timer is similar to the protection timer used in PSTN/ISDN. The timer value range is between 5 and 15 seconds, and the default value is 10 seconds.

The procedures for collecting additional digits are described in subclauses N.3.2 and N.3.3. When end of address signalling has been determined, the en-bloc conversion function shall generate an INVITE request, add all digits to the request and forwards the request towards its destination.

### N.3.2 Multiple-INVITE method

Upon reception of an INVITE request, the en-bloc conversion function shall:

- 1) if an inter digit timer is running for a previously received INVITE request with the same Call-ID and From header, and
  - a) if the number of digits within that previous INVITE request is below the number of digits received in the new INVITE request (or as an equivalent test if the CSeqID of the previous INVITE request is below the CSeqID

of the new INVITE request), stop the inter-digit timer for that previous INVITE request and send a 484 (Address Incomplete) response for it; and

- b) if the number of digits with the previous INVITE request is above or equal to the number of digits received in the new INVITE request (or as an equivalent test if the CSeqID of the previous INVITE request is below the CSeqID of the new INVITE request), send a 484 (Address Incomplete) response for the new INVITE request; and
- 2) if the en-bloc conversion function determines that the number received in the INVITE request is complete, forward the INVITE request; and
- 3) if the en-bloc conversion function determines that it will not be able to forward the request even if additional digits are received, send a 404 (Not Found) response; and
- 4) if the en-bloc conversion function chooses to collect additional digits, store the INVITE request and start an inter-digit timer to wait for possible INVITE requests with the same Call ID and From header.

When the inter-digit timer expires the en-bloc conversion function shall:

- 1) if it determines that the number received in the stored INVITE request is incomplete (e. g. by number analysis), terminate the call setup by sending a 484 (Address Incomplete) response towards the sender of the INVITE request; and
- 2) if it does not determine that the number received in the last INVITE request is incomplete, forward the corresponding stored INVITE request to the next hop.

After forwarding an INVITE request, the en-bloc conversion function shall apply SIP proxy procedures for all subsequent SIP messages within the corresponding dialogue, unless other functionality not related to en-bloc conversion allocated in the same physical node requires a different behaviour.

### N.3.3 In-dialog method

Upon receiving an initial INVITE request carrying an SDP offer, the en-bloc conversion function shall:

- 1) if it determines that the request contains a complete number, forward the request towards its destination;
- 2) if the en-bloc conversion function chooses to collect additional digits in INFO requests before forwarding the request, and the sender of the INVITE request has indicated support of reliable responses, store the received digits, send a reliable 183 (Session Progress) provisional response without an SDP answer in order to establish an early dialog with the sender of the INVITE request, and start an inter digit timer; or
- 3) if the en-bloc conversion function determines that it will not be able to forward the request even if additional digits are received, send a 404 (Not Found) response.

Upon receiving an initial INVITE request without an SDP offer, the en-bloc conversion function shall:

- 1) if it is determined that the request contains a complete number, forward the request towards its destination; or
- 2) send a 404 (Not Found) response.

**NOTE:** If the initial INVITE request does not contain an SDP offer, a reliable 18x provisional response generated by the en-bloc conversion function would have to contain an SDP offer. The en-bloc conversion function for the in-dialog method specified here does not support en-bloc conversion for calls with an initial INVITE request that does not contain an SDP offer in the present release. However, en-bloc conversion for an initial INVITE request that does not contain an SDP offer can be performed by the originating SIP entity (e.g. MGCF).

Upon receiving an INFO request carrying additional digits, and an early dialog towards the destination of the initial SIP INVITE request for the call has not been created, the en-bloc conversion function shall:

- 1) send a 200 (OK) response to the INFO request;
- 2) add the received digits to the previously stored digits for the call;
- 3) re-start the inter digit timer; and

- 4) check if it can determine that a complete number for the call has been received.

When the en-bloc conversion function determines that a complete number for the call has been received, it shall add all stored digits to the initial INVITE request and forward the request towards its destination and stop the inter digit timer.

When the inter-digit timer expires the en-bloc conversion function shall

- 1) if it determines that the number so far is incomplete (e. g. by number analysis), terminate the call setup by sending a 484 (Address Incomplete) response towards the sender of the INVITE request; or
- 2) if it does not determine that the number received in the last INVITE request is incomplete, forward the INVITE request to the next hop, including all received digits.

Upon receiving an INFO request carrying additional digits, if the en-bloc conversion function has forwarded the initial INVITE request towards its destination, the en-bloc conversion function shall send a 200 (OK) response to the INFO request and not forward the INFO request.

Apart from INFO requests carrying additional digits received after the initial INVITE request has been forwarded, the en-bloc conversion function shall forward all SIP messages.

The en bloc conversion function will receive a "tag" To header field parameter value from the receiver of the initial INVITE request, which is different from the "tag" To header field parameter value that the digit collection function inserted in the 183 (Session Progress) response that it sent when it received the initial INVITE request. The digit collection function shall modify the "tag" To header field parameter value accordingly when forwarding in-dialog SIP messages.



---

# Annex O (normative): IP-Connectivity Access Network specific concepts when using the EPC via cdma2000<sup>®</sup> HRPD to access IM CN subsystem

## O.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is the Evolved Packet Core (EPC) via a cdma2000<sup>®</sup> HRPD access network.

---

## O.2 IP-CAN aspects when connected to the IM CN subsystem

### O.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by the EPC and cdma2000<sup>®</sup> HRPD access network as specified by 3GPP2 X.P0057 [86C] to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the UE on the use of these packet-mode services are specified in this clause. Requirements for the P-GW in support of this communication are specified in 3GPP TS 29.061 [11] and 3GPP TS 29.212 [13B].

Requirements for the use of the EPC via packet cdma2000<sup>®</sup> HRPD as an IP-CAN are specified in 3GPP2 X.P0057 [86C].

### O.2.2 Procedures at the UE

#### O.2.2.1 IP-CAN bearer context activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

- a) establish a connection with the the IP-CAN via the cdma2000<sup>®</sup> HRPD wireless IP network specified in 3GPP2 X.P0057 [86C]. Upon establishing a connection with the cdma2000<sup>®</sup> eHRPD wireless IP network, the UE can have an IPv4 address only, an IPv6 address only, or both IPv4 and IPv6 addresses simultaneously;
- b) ensure that a IP-CAN bearer context used for SIP signalling is available, according to the APN and P-GW selection criteria described in 3GPP TS 23.402 [7E]. This IP-CAN bearer context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration;

NOTE 1: Any IP-CAN bearer can carry both IM CN subsystem signalling and media if the media does not need to be authorized by Policy and Charging control mechanisms as defined in 3GPP TS 29.212 [13B], and the media stream is not mandated by the P-CSCF to be carried in a separate IP-CAN bearer.

NOTE 2: IP-CAN PDN connection and bearer management procedures are specified in 3GPP2 X.P0057 [86C].

- c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

- I. Use DHCP mechanism
- II Retrieve the list of P-CSCF address(es) stored in the IMC
- III Obtain the list of P-CSCFaddress(es) from the IMS management object

#### IV. Transfer P-CSCF address(es) within the IP-CAN bearer context activation procedure.

The UE shall indicate the request for a P-CSCF address to the network within the Protocol Configuration Options information element of the during PDN connectivity establishment as specified in 3GPP2 X.P0057 [86C].

If the network provides the UE with a list of P-CSCF IPv4 or IPv6 addresses, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options information element as the P-CSCF address with the highest priority.

The UE can freely select method I, II, III, or IV for P-CSCF discovery. If DHCP is used, the following procedures apply:

Upon establishing an IP-CAN bearer, the UE may use the Dynamic Host Configuration Protocol (DHCP) specified in RFC 2131 [40A] or Dynamic Host Configuration Protocol for IPv6 (DHCPv6) specified in RFC 3315 [40] to discover the P-CSCF.

Prior to accessing the DHCP server, the UE will have obtained an IP address via means other than DHCP and DHCPv6.

If the UE uses DHCP for P-CSCF discovery and the UE is unaware of the address of the DHCP server, the UE shall send the DHCPINFORM using the limited broadcast IP address (i.e., 255.255.255.255) and UDP port 67. If the UE knows the IP address of the DHCP server, the UE shall send the DHCPINFORM to the DHCP server's unicast IP address and UDP port 67. The DHCP server shall send the DHCPACK on the IP address specified in the Client IP Address field of the DHCPINFORM. The DHCP server may include, in the DHCPACK, the SIP Server DHCP Option specified in RFC 3361 [35A], which carries either a list of IPv4 address(es) of the P-CSCF(s) or a list of DNS fully qualified domain name(s) that can be mapped to one or more P-CSCF(s). If the UE uses DHCPv6 for P-CSCF discovery and the UE is unaware of the address of the DHCP Server, the UE shall send an Information Request using the IPv6 multicast address FF02::1:2 and the UDP port 547. If the UE knows the IP address of the DHCPv6 server, the UE shall send the Information Request message to the DHCPv6 server's IP address and UDP port 547. In the Information Request, the UE may request either one or both the SIP Servers Domain Name List option and the SIP Servers IPv6 Address List option specified in RFC 3319 [41]. The DHCP server shall send the Reply to the IP address specified in the Information Request. The DHCP server may include in the Reply either one or both the SIP Servers Domain Name List option and the SIP Servers IPv6 Address List option, as requested by the UE.

In case several P-CSCF's IP addresses or domain names are provided to the UE, the UE shall perform P-CSCF selection according to RFC 3361 [35A] or RFC 3319 [41]. The UE shall perform the procedure for the resolution of domain name according to RFC 3263 [27A].

### O.2.2.1A Modification of an IP-CAN bearer context used for SIP signalling

The UE shall not modify the IP-CAN bearer from being used exclusively for SIP signalling to a general purpose IP-CAN bearer and vice versa.

After the establishment of a SIP bearer context used for SIP signalling, the UE shall not indicate the request for a P-CSCF address to the network when requesting an IP-CAN bearer modification for that APN. The UE shall ignore P-CSCF address(es) if received from the network as part of the bearer modification procedure.

### O.2.2.1B Re-establishment of the IP-CAN bearer context for SIP signalling

If the IP-CAN bearer context for SIP signalling is lost and cannot be re-established:

- a. if the SIP signalling was carried over a dedicated IP-CAN bearer, the UE shall release all resources established as a result of SIP signalling by either:
  - requesting an IP-CAN bearer modification if there are IP-CAN bearers to this PDN that are not related SIP sessions; or
  - initiating disconnection of the PDN connection if all the bearers to this PDN are related to SIP sessions.

**NOTE:** If the SIP signalling was carried over the default IP-CAN bearer, all the resources established as a result of SIP signalling are released.

## O.2.2.1 CP-CSCF restoration procedure

A UE supporting the P-CSCF restoration procedure performs one of the following procedures:

- A if the UE used method II for P-CSCF discovery and if the UE receives one or more P-CSCF address(es) in an VSNCP Configure-Request message and the one or more P-CSCF address(es) do not include the address of the currently used P-CSCF, then the UE shall acquire a different P-CSCF address from the one or more P-CSCF address(es) in the VSNCP Configure-Request message. The UE shall assume that the more than one P-CSCF address are prioritised with the first P-CSCF address within the Protocol Configuration Options information element as the P-CSCF address with the highest priority;
- B if the UE uses RFC 6223 [143] as part of P-CSCF restoration procedures, and if the P-CSCF fails to respond to a keep-alive request, then the UE shall acquire a different P-CSCF address using one of the methods I, II and III for P-CSCF discovery described in the subclause O.2.2.1.

When a different P-CSCF address is acquired the UE shall perform an initial registration as specified in subclause 5.1.

## O.2.2.2 Session management procedures

The existing procedures for session management as described in 3GPP2 X.P0057 [86C] shall apply while the UE is connected to the IM CN subsystem.

## O.2.2.3 Mobility management procedures

The existing procedures for mobility management as described in 3GPP2 X.P0057 [86C] shall apply while the UE is connected to the IM CN subsystem.

## O.2.2.4 Cell selection and lack of coverage

The existing mechanisms and criteria for cell selection as described in 3GPP2 C.S0014-C [86D] shall apply while the UE is connected to the IM CN subsystem.

## O.2.2.5 IP-CAN bearer contexts for media

### O.2.2.5.1 General requirements

NOTE 1: The UE cannot control whether media streams belonging to different SIP sessions are established on the same IP-CAN bearer context or not. During establishment of a session, the UE establishes data stream(s) for media related to the session. Such data stream(s) can result in activation of additional IP-CAN bearer context(s). Either the UE or the network can request for resource allocations for media, but the establishment and modification of the IP-CAN bearer is controlled by the network as described in 3GPP2 X.P0057 [86C].

NOTE 2: When the UE wishes to allocate bandwidth for RTP and RTCP, the rules as outlined in 3GPP TS 29.213 [13C] apply. Application of QoS to when using an EPC IP-CAN with cdma2000® HRPD is described in 3GPP2 X.P0057 [86C].

#### O.2.2.5.1A Activation or modification of IP-CAN bearer contexts for media by the UE

No additional clarifications are needed for the use of the EPC via cdma2000® HRPD as an IP-CAN.

#### O.2.2.5.1B Activation or modification of IP-CAN bearer contexts for media by the network

If the UE receives an activation request from the network for an IP-CAN bearer context which is associated with the IP-CAN bearer context used for signalling, the UE shall, based on the information contained in the Traffic Flow Template provided by the network, correlate the media IP-CAN bearer context with a currently ongoing SIP session establishment or SIP session modification.

If the UE receives a modification request from the network for an IP-CAN bearer context that is used for one or more media streams in an ongoing SIP session, the UE shall modify the related IP-CAN bearer context in accordance with the request received from the network.

### O.2.2.5.1C Deactivation of of IP-CAN bearer contexts for media

Not applicable

### O.2.2.5.2 Special requirements applying to forked responses

NOTE 1: The procedures in this subclause only apply when the UE requests activation and modification of media bearers. In the case where the network activates and modifies the media bearers the network takes care of the handling of media bearers in the case of forking.

Since the UE does not know that forking has occurred until a second, provisional response arrives, the UE requests resource allocation as required by the initial response received. If a subsequent provisional response is received, different alternative actions may be performed depending on the requirements in the SDP answer:

- 1) the bearer requirements of the subsequent SDP can be accommodated by the existing resources requested. The UE performs no further resource requests.
- 2) the subsequent SDP introduces different QoS requirements or additional IP flows. The UE requests further resource allocation according to subclause O.2.2.5.1.
- 3) the subsequent SDP introduces one or more additional IP flows. The UE requests further resource allocation according to subclause O.2.2.5.1.

NOTE 2: When several forked responses are received, the resources requested by the UE are the "logical OR" of the resources indicated in the multiple responses to avoid allocation of unnecessary resources. The UE does not request more resources than proposed in the original INVITE request.

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall release all the unneeded IP-CAN resources. Therefore, upon the reception of the first final 200 (OK) response for the INVITE request (in addition to the procedures defined in RFC 3261 [26] subclause 13.2.2.4), the UE shall:

- 1) in case resources were established or modified as a consequence of the INVITE request and forked provisional responses that are not related to the accepted 200 (OK) response, send release request to release the unneeded resources.

### O.2.2.5.3 Unsuccessful situations

Not applicable.

### O.2.2.6 Emergency service

Emergency services is not supported when the IP-CAN is the EPC via a cdma2000® HRPD access network.

---

## O.2A Usage of SDP

### O.2A.0 General

Not applicable.

### O.2A.1 Impact on SDP offer / answer of activation or modification of IP-CAN bearer context for media by the network

If, due to the activation of an IP-CAN bearer context from the network the related SDP media description needs to be changed the UE shall update the related SDP information by sending a new SDP offer within a SIP request, which is sent over the existing SIP dialog,

If the UE receives a modification request from the network for an IP-CAN bearer context that is used for one or more media streams in an ongoing SIP session, the UE shall:

- 1) if, due to the modification of the IP-CAN bearer context, the related SDP media description need to be changed, update the related SDP information by sending a new SDP offer within a SIP request, that is sent over the existing SIP dialog, and respond to the IP-CAN bearer context modification request.

NOTE: The UE can decide to indicate additional media streams as well as additional or different codecs in the SDP offer than those used in the already ongoing session.

## O.2A.2 Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE

If the UE receives an SDP offer where the SDP offer includes all media streams for which the originating side indicated its local preconditions as met, if the precondition mechanism is supported by the terminating UE and the IP-CAN performs network-initiated resource reservation for the terminating UE and the available resources are not sufficient for the received offer the terminating UE shall indicate its local preconditions and provide the SDP answer to the originating side without waiting for resource reservation.

NOTE: If the resource reservation is controlled by the network, the resource reservation request is initiated by the network after the P-CSCF has authorised the respective IP flows and provided the QoS requirements over the Rx interface to the PCRF as described in 3GPP TS 29.214 [13D].

## O.2A.3 Emergency service

No additional procedures defined.

---

# O.3 Application usage of SIP

## O.3.1 Procedures at the UE

### O.3.1.1 P-Access-Network-Info header field

The UE shall always include the P-Access-Network-Info header field where indicated in subclause 5.1.

### O.3.1.2 Availability for calls

Not applicable.

### O.3.1.2A Availability for SMS

Void.

### O.3.1.3 Authorization header field

When using SIP digest or SIP digest without TLS, the UE need not include an Authorization header field on sending a REGISTER request, as defined in subclause 5.1.1.2.1.

NOTE: In case the Authorization header field is absent, the mechanism only supports that one public user identity is associated with only one private user identity. The public user identity is set so that it is possible to derive the private user identity from the public user identity by removing SIP URI scheme and the following parts of the SIP URI if present: port number, URI parameters, and To header field parameters. Therefore, the public user identity used for registration in this case cannot be shared across multiple UEs. Deployment scenarios that require public user identities to be shared across multiple UEs that don't include an private user identity in the initial REGISTER request can be supported as follows:

- Assign each sharing UE a unique public user identity to be used for registration,
- Assign the shared public user identities to the implicit registration set of the unique registering public user identities assigned to each sharing UE.

- O.3.1.4 SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE

Not applicable.

## O.3.2 Procedures at the P-CSCF

### O.3.2.1 Determining network to which the originating user is attached

The P-CSCF handling is as defined in subclause M.3.2.

NOTE: Emergency call support for the EPC IP-CAN is not specified in this release. A common P-Access-Network-Info header field value is used for both cdma2000<sup>®</sup> HRPD based IP-CANs (i.e. HRPD access specified by 3GPP2 X.S0011-E [127], and HRPD access as specified by 3GPP2 X.P0057 [86C]). The result of this is that in both cases the handling in the P-CSCF must be identical. If an operator deploys an IM CN subsystem with both cdma2000<sup>®</sup> HRPD based IP-CANs, the P-CSCF has no means of distinguishing one from the other. The emergency call handling for the EPC IP-CAN using cdma2000<sup>®</sup> HRPD access as specified by 3GPP2 X.P0057 [86C] is out of scope for this release of this specification, and therefore all identified emergency calls with a P-Access-Network-Info header field value of "3GPP2-1X-HRPD" will be handled with a 380 (Alternative Service) response when HRPD IP-CAN emergency support is not active.

### O.3.2.2 Location information handling

Void.

## O.3.3 Procedures at the S-CSCF

The S-CSCF handling is as defined in subclause M.3.3.

---

## O.4 3GPP specific encoding for SIP header field extensions

### O.4.1 Void

---

## O.5 Use of circuit-switched domain

There is no CS domain in this access technology.

Annex P (informative):  
Void

---

## Annex Q (normative): IP-Connectivity Access Network specific concepts when using the cdma2000<sup>®</sup> 1x Femtocell Network to access IM CN subsystem

### Q.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is an IP network as incorporated into the cdma2000<sup>®</sup> 1x femtocell network subsystem [86E].

---

### Q.2 cdma2000<sup>®</sup> 1x Femtocell Network aspects when connected to the IM CN subsystem

#### Q.2.1 Introduction

In the cdma2000<sup>®</sup> 1x femtocell network subsystem, the cdma2000<sup>®</sup> 1x Mobile Station (MS) accesses the IM CN subsystem by utilising the services provided by the cdma2000<sup>®</sup> 1x Femtocell Access Point (FAP) [86E].

NOTE: Protocol between the cdma2000<sup>®</sup> 1x MS and the cdma2000<sup>®</sup> 1x FAP is out of scope of this document.

The cdma2000<sup>®</sup> 1x FAP 3GPP2 X.P0059-200 [86E] acts as a UE toward the IM CN subsystem.

From the perspective of the FAP, it is assumed that one or more IP-CAN bearer(s) are provided, in the form of connection(s) managed by the layer 2.

#### Q.2.2 Procedures at the UE

##### Q.2.2.1 Activation and P-CSCF discovery

Unless a static IP address is allocated to the cdma2000<sup>®</sup> 1x FAP, prior to communication with the IM CN subsystem, the cdma2000<sup>®</sup> 1x FAP shall perform a Network Attachment procedure depending on the used cdma2000<sup>®</sup> 1x FAP access type. When using a cdma2000<sup>®</sup> 1x FAP access, both IPv4 and IPv6 may be used to access the IM CN subsystem. The cdma2000<sup>®</sup> 1x FAP may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or a DNS Server IPv6 address(es) via RFC 3315 [40].

When using IPv4, the cdma2000<sup>®</sup> 1x FAP may acquire a P-CSCF address(es) by using the DHCP (see RFC 2132 [20F]), the DHCPv4 options for SIP servers (see RFC 3361 [35A]), and RFC 3263 [27A].

In case the DHCP server provides several P-CSCF addresses or FQDNs to the cdma2000<sup>®</sup> 1x FAP, the cdma2000<sup>®</sup> 1x FAP shall select the P-CSCF address or FQDN as indicated in RFC 3361 [35A]. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the cdma2000<sup>®</sup> 1x FAP is implementation specific.

When using IPv6, the cdma2000<sup>®</sup> 1x FAP may acquire a P-CSCF address(es) by using the DHCPv6 (see RFC 3315 [40] and RFC 3646 [56C]), the DHCPv6 options for SIP servers (see RFC 3319 [41]), and RFC 3263 [27H].

In case the DHCP server provides several P-CSCF addresses or FQDNs to the cdma2000<sup>®</sup> 1x FAP, the cdma2000<sup>®</sup> 1x FAP shall select the P-CSCF address or FQDN as indicated in RFC 3319 [41]. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the cdma2000<sup>®</sup> 1x FAP is implementation specific.

##### Q.2.2.1A Modification of IP-CAN used for SIP signalling

Not applicable.



### Q.2.2.1B Re-establishment of IP-CAN used for SIP signalling

Not applicable.

#### Q.2.2.2 Void

#### Q.2.2.3 Void

#### Q.2.2.4 Void

### Q.2.2.5 Handling of the IP-CAN for media

#### Q.2.2.5.1 General requirements

The cdma2000<sup>®</sup> 1x FAP uses the bearer used for signalling also for transmission of media.

##### Q.2.2.5.1A Activation or modification of IP-CAN for media by the UE

Not applicable.

##### Q.2.2.5.1B Activation or modification of IP-CAN for media by the network

Not applicable.

##### Q.2.2.5.1C Deactivation of IP-CAN for media

Not applicable

#### Q.2.2.5.2 Special requirements applying to forked responses

Not applicable.

#### Q.2.2.5.3 Unsuccessful situations

Not applicable.

### Q.2.2.6 Emergency service

Emergency calls are perceived as regular calls from the perspective of the IM CN subsystem. Entities outside the IM CN subsystem identify and route such calls to PSAP.

## Q.2A Usage of SDP

### Q.2A.0 General

Not applicable.

#### Q.2A.1 Impact on SDP offer / answer of activation or modification of IP-CAN for media by the network

Not applicable.

#### Q.2A.2 Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE

Not applicable.

## Q.2A.3 Emergency service

No additional procedures defined.

---

## Q.3 Application usage of SIP

### Q.3.1 Procedures at the UE

#### Q.3.1.1 P-Access-Network-Info header field

The cdma2000<sup>®</sup> 1x FAP shall include the P-Access-Network-Info header field where indicated in subclause 5.1.

#### Q.3.1.2 Availability for calls

Not applicable.

#### Q.3.1.2A Availability for SMS

Void.

#### Q.3.1.3 Authorization header field

Void.

#### Q.3.1.4 SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE

Not applicable.

### Q.3.2 Procedures at the P-CSCF

#### Q.3.2.1 Determining network to which the originating user is attached

If access-type field in the P-Access-Network-Info header field indicated 3GPP2-1X-Femto access the P-CSCF shall assume that an initial request for a dialog or standalone transaction or an unknown method destined for a PSAP is initiated in the same country.

#### Q.3.2.2 Location information handling

Not applicable

### Q.3.3 Procedures at the S-CSCF

#### Q.3.3.1 Notification of AS about registration status

Not applicable

---

## Q.4 3GPP specific encoding for SIP header field extensions

Void.

## Q.5 Use of circuit-switched domain

Not applicable

---

# Annex R (normative): IP-Connectivity Access Network specific concepts when using the EPC via WLAN to access IM CN subsystem

## R.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IM CN subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is the Evolved Packet Core (EPC) via Wireless Local Access Network (WLAN).

---

## R.2 IP-CAN aspects when connected to the IM CN subsystem

### R.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by the EPC and the WLAN to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the UE on the use of these packet-mode services are specified in this clause.

### R.2.2 Procedures at the UE

#### R.2.2.1 Establishment of IP-CAN bearer and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

NOTE: The UE performs access network discovery and selection procedures as specified in 3GPP TS 24.302 [8U] and executes access authentication signalling for access to the EPC between the UE and 3GPP AAA server, if applicable, as described in 3GPP TS 24.302 [8U] prior to perform the procedure to obtain a local IP address;

- a) obtain a local IP address from the untrusted non 3GPP access network and establish an IKEv2 security association and an IPsec ESP security association with ePDG, if the UE attaches to the EPC via untrusted WLAN IP access on S2b. The UE can determine trust relationship of a non-3GPP IP access network as specified in 3GPP TS 24.302 [8U]. Furthermore, the UE accessing from the untrusted WLAN or trusted WLAN on S2c shall obtain a local IP address and establish an IKEv2 security association and an IPsec ESP security association as described in 3GPP TS 24.302 [8U] and 3GPP TS 24.303 [8V]. If the UE supports the Fixed Access Broadband interworking, the establishment of tunnel specified in 3GPP TS 24.139 [8X] shall be applied. The IKEv2 security association and the IPsec ESP security association (tunnel) shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration;

The UE may carry both signalling and media on an IPsec ESP security association.

If the UE attaches to the EPC via S2a on a trusted WLAN access network, the IPv4 address and/or IPv6 prefix is allocated as specified in 3GPP TS 24.302 [8U]. The UE IP address shall remain valid throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration;

- b) Acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

- I. Use DHCP mechanism
- II. Use DNS

When using IPv4, the UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F]. When using IPv6, the UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C].

### III. Obtain the list of P-CSCF address(es) from the IMS management object

The UE can freely select method I, II, or III for P-CSCF discovery. If DHCP is used, the following procedures apply:

Upon establishing an IP-CAN, the UE may use the Dynamic Host Configuration Protocol (DHCP) specified in RFC 2131 [40A] or Dynamic Host Configuration Protocol for IPv6 (DHCPv6) specified in RFC 3315 [40] to discover the P-CSCF.

Prior to accessing the DHCP server, the UE will have obtained an IP address via means other than DHCP and DHCPv6.

If the UE uses DHCP for P-CSCF discovery and the UE is unaware of the address of the DHCP server, the UE sends the DHCPINFORM using the limited broadcast IP address (i.e., 255.255.255.255) and UDP port 67. If the UE knows the IP address of the DHCP server, the UE shall send the DHCPINFORM to the DHCP server's unicast IP address and UDP port 67. The DHCP server sends the DHCPACK on the IP address specified in the Client IP Address field of the DHCPINFORM. The DHCP server can include, in the DHCPACK, the SIP Server DHCP Option specified in RFC 3361 [35A], which carries either a list of IPv4 address(es) of the P-CSCF(s) or a list of DNS fully qualified domain name(s) that can be mapped to one or more P-CSCF(s). If the UE uses DHCPv6 for P-CSCF discovery and the UE is unaware of the address of the DHCP Server, the UE shall send an Information Request using the IPv6 multicast address FF02::1:2 and the UDP port 547. If the UE knows the IP address of the DHCPv6 server, the UE shall send the Information Request message to the DHCPv6 server's IP address and UDP port 547. In the Information Request, the UE can request either one or both the SIP Servers Domain Name List option and the SIP Servers IPv6 Address List option specified in RFC 3319 [41]. The DHCP server sends the Reply to the IP address specified in the Information Request. The DHCP server can include in the Reply either one or both the SIP Servers Domain Name List option and the SIP Servers IPv6 Address List option, as requested by the UE.

In case several P-CSCF's IP addresses or domain names are provided to the UE, the UE shall perform P-CSCF selection according to RFC 3361 [35A] or RFC 3319 [41]. The UE shall perform the procedure for the resolution of domain name according to RFC 3263 [27A]. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

#### R.2.2.1A Modification of an IP-CAN used for SIP signalling

Not applicable.

#### R.2.2.1B Re-establishment of the IP-CAN used for SIP signalling

Not applicable.

#### R.2.2.1C P-CSCF restoration procedure

A UE supporting the P-CSCF restoration procedure uses the keep-alive procedures described in RFC 6223 [143].

If the P-CSCF fails to respond to keep-alive requests the UE shall acquire a different P-CSCF address using any of the methods described in the subclause R.2.2.1 and perform an initial registration as specified in subclause 5.1.

#### R.2.2.2 Void

#### R.2.2.3 IP-CAN support of DHCP based P-CSCF discovery

When using S2c to access the EPC via WLAN, the Home Agent (HA) in case of Mobile IP with reverse tunneling, can forward the packet to one or more local DHCP servers, or relay the packet to a specific DHCP server. The HA in case of Mobile IP with reverse tunnelling, does not forward the DHCPINFORM (or Information-Request) to any UE.

NOTE 1: For forwarding the DHCPINFORM or Information-Request, the HA in case of Mobile IP with reverse tunnelling, does not change the destination IP address of the packet.

NOTE 2: For relaying the DHCPINFORM or Information-Request, the HA in case of Mobile IP with reverse tunnelling inserts a DHCP server's IP address in the destination IP address field of the packet.

## R.2.2.4 Void

## R.2.2.5 Tunnel procedures for media

### R.2.2.5.1 General requirements

The UE can establish media streams that belong to different SIP sessions on the same tunnel when accessing the EPC via untrusted WLAN.

During establishment of a session, the UE establishes data streams(s) for media related to the session. When using S2c to access the EPC via untrusted WLAN, such data stream(s) may result in activation of additional IPsec ESP security associations (tunnels).

If the capabilities of the originating UE, or operator policy at the ePDG prevents the originating UE from establishment of additional IPsec ESP security associations (tunnels) according to the media grouping attributes given by the P-CSCF in accordance with RFC 3524 [54], the UE will not establish such grouping of media streams. Instead, the originating UE shall negotiate media parameters for the session according to RFC 3264 [27B].

If the capabilities of the terminating UE or operator policy at the ePDG prevents the originating UE from establishment of additional IPsec ESP security associations (tunnels) according to the media grouping attributes given by the P-CSCF in accordance with RFC 3524 [54], the UE will not establish such grouping of media streams. Instead, the terminating UE shall handle such SDP offers in accordance with RFC 3388 [53].

The UE can receive a media authorization token in the P-Media-Authorization header field from the P-CSCF according to RFC 3313 [31]. If a media authorization token is received in the P-Media-Authorization header field when a SIP session is initiated, the UE shall reuse the existing tunnel and ignore the media authorization token.

#### R.2.2.5.1A Modification of tunnel for media by the UE

The tunnel modification procedure for the UE shall follow the procedures specified in 3GPP TS 24.302 [8U]. If the UE supports the Fixed Access Broadband interworking, the modification of tunnel specified in 3GPP TS 24.139 [8X] shall be applied.

#### R.2.2.5.1B Modification of tunnel for media by the network

The UE shall follow the procedure specified in 3GPP TS 24.302 [8U] for the modification of tunnel. If the UE supports the Fixed Access Broadband interworking, the modification of tunnel specified in 3GPP TS 24.139 [8X] shall be applied.

#### R.2.2.5.1C Deactivation of tunnel for media

Not applicable.

### R.2.2.5.2 Special requirements applying to forked responses

Since the UE is unable to perform bearer modification, forked responses place no special requirements on the UE.

### R.2.2.5.3 Unsuccessful situations

Not applicable.

## R.2.2.6 Emergency service

Emergency bearers are not supported when the IP-CAN is the EPC via WLAN.

---

## R.2A Usage of SDP

### R.2A.0 General

Not applicable.

## R.2A.1 Impact on SDP offer / answer of activation or modification of IP-CAN for media by the network

Not applicable.

## R.2A.2 Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE

Not applicable.

## R.2A.3 Emergency service

No additional procedures defined.

---

# R.3 Application usage of SIP

## R.3.1 Procedures at the UE

### R.3.1.1 P-Access-Network-Info header field

The UE shall always include the P-Access-Network-Info header field where indicated in subclause 5.1.

### R.3.1.2 Availability for calls

Not applicable.

### R.3.1.2A Availability for SMS

Void.

### R.3.1.3 Authorization header field

When using SIP digest or SIP digest without TLS, the UE need not include an Authorization header field on sending a REGISTER request, as defined in subclause 5.1.1.2.1.

**NOTE:** In case the Authorization header field is absent, the mechanism only supports that one public user identity is associated with only one private user identity. The public user identity is set so that it is possible to derive the private user identity from the public user identity by removing SIP URI scheme and the following parts of the SIP URI if present: port number, URI parameters, and To header field parameters. Therefore, the public user identity used for registration in this case cannot be shared across multiple UEs. Deployment scenarios that require public user identities to be shared across multiple UEs that don't include an private user identity in the initial REGISTER request can be supported as follows:

- Assign each sharing UE a unique public user identity to be used for registration,
- Assign the shared public user identities to the implicit registration set of the unique registering public user identities assigned to each sharing UE.

### R.3.1.4 SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE

Not applicable.

## R.3.2 Procedures at the P-CSCF

### R.3.2.1 Determining network to which the originating user is attached

NOTE: This version of the specification does not specify any procedures to determine the originating network of the WLAN AP.

### R.3.2.2 Location information handling

Void.

## R.3.3 Procedures at the S-CSCF

### R.3.3.1 Notification of AS about registration status

Not applicable.

---

## R.4 3GPP specific encoding for SIP header field extensions

Void.

---

## R.5 Use of circuit-switched domain

Void.



---

# Annex S (normative): IP-Connectivity Access Network specific concepts when using DVB-RCS2 to access IM CN subsystem

## S.1 Scope

The present annex defines IP-CAN specific requirements for a call control protocol for use in the IP Multimedia (IM) Core Network (CN) subsystem based on the Session Initiation Protocol (SIP), and the associated Session Description Protocol (SDP), where the IP-CAN is DVB-RCS2 satellite access network.

DVB-RCS2 (Second Generation DVB Interactive Satellite System) is a term referring to the ETSI standard ETSI TS 101 454-1 [193], ETSI EN 301 545-2 [194], ETSI TS 101 545-3 [195] for 2<sup>nd</sup> generation DVB satellite based access network technology with a return channel for two-way communication.

---

## S.2 DVB-RCS2 aspects when connected to the IM CN subsystem

### S.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by the DVB-RCS2 satellite access network to provide packet-mode communication between the UE and the IM CN subsystem.

From the perspective of the UE, the necessary IP-CAN bearer for signalling is transparently available to the UE.

The UE is not directly involved in requests for IP-CAN bearer(s) for media flow(s). The IM CN interacts with the PCRF in the DVB-RCS2 IP-CAN to establish IP-CAN bearer(s) for media flow(s), on behalf of the UE.

### S.2.2 Procedures at the UE

#### S.2.2.1 Activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

- a) establish a connection to a DVB-RCS2 RCST depending on local configuration; the RCST shall have completed the RCST commissioning and initialization procedures as described in ETSI TS 101 545-3 [195], and thus have achieved IP connectivity to the NCC of an SVN;
- b) obtain an IP address using the standard IETF protocols (e.g., DHCP or IPCP). The UE shall fix the obtained IP address throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the last deregistration; and
- c) acquire a P-CSCF address(es), according to one of the methods described in subclause 9.2.1; the method available to the UE is determined by the SVN to which the RCST is connected.

#### S.2.2.1A Modification of IP-CAN bearer used for SIP signalling

Not applicable.

#### S.2.2.1B Re-establishment of IP-CAN bearer used for SIP signalling

Not applicable.

#### S.2.2.1C P-CSCF restoration procedure

A UE supporting the P-CSCF restoration procedure uses the keep-alive procedures described in RFC 6223 [143].

If the P-CSCF fails to respond to keep-alive requests the UE shall acquire a different P-CSCF address using any of the methods described in the subclause S.2.2.1 and perform an initial registration as specified in subclause 5.1.

### S.2.2.2 Void

### S.2.2.3 Void

### S.2.2.4 Void

## S.2.2.5 Handling of the IP-CAN for media

### S.2.2.5.1 General requirements

The UE does not directly request resources for media flow(s).

#### S.2.2.5.1A Activation or modification of IP-CAN for media by the UE

Not applicable.

#### S.2.2.5.1B Activation or modification of IP-CAN for media by the network

Not applicable.

#### S.2.2.5.1C Deactivation of IP-CAN for media

Not applicable.

### S.2.2.5.2 Special requirements applying to forked responses

The UE does not directly request resources for media flow(s). As a result there are no special UE requirements applying to forked responses.

### S.2.2.5.3 Unsuccessful situations

Not applicable.

## S.2.2.6 Emergency service

Emergency service is not supported when the IP-CAN is a DVB-RCS2 satellite access network.

---

## S.2A Usage of SDP

### S.2A.0 General

Not applicable.

### S.2A.1 Impact on SDP offer / answer of activation or modification of satellite bearer for media by the network

Not applicable.

### S.2A.2 Handling of SDP at the terminating UE when originating UE has resources available and IP-CAN performs network-initiated resource reservation for terminating UE

Not applicable.

## S.2A.3 Emergency service

No additional procedures defined.

---

## S.3 Application usage of SIP

### S.3.1 Procedures at the UE

#### S.3.1.1 P-Access-Network-Info header field

The UE may, but need not, include the P-Access-Network-Info header field where indicated in subclause 5.1.

#### S.3.1.2 Availability for calls

Not applicable.

#### S.3.1.2A Availability for SMS

Void.

#### S.3.1.3 Authorization header field

Void

#### S.3.1.4 SIP handling at the terminating UE when precondition is not supported in the received INVITE request, the terminating UE does not have resources available and IP-CAN performs network-initiated resource reservation for the terminating UE

Not applicable.

### S.3.2 Procedures at the P-CSCF

#### S.3.2.1 Determining network to which the originating user is attached

In order to determine from which network the request was originated the P-CSCF shall check if the location information received in the network provided and/or UE provided "dvb-rcs2-node-id" parameter in the P-Access-Network-Info header field(s) indicates that the UE is connected to the same network as the P-CSCF or not.

NOTE 1: If local policy does not require the insertion of P-Access-Network-Info header field in the P-CSCF even if it is missing in the received initial request, the P-CSCF can assume that the request is initiated by a UE in the same network as the P-CSCF.

NOTE 2: If the location information in the network provided and UE provided "dvb-rcs2-node-id" parameters (in a request that includes two P-Access-Network-Info header fields) is contradictory, or the two P-Access-Network-Info header fields indicate different access types the P-CSCF ignores either the network provided or the UE provided information according to operator policy.

#### S.3.2.2 Location information handling

Upon receipt of an initial request for a dialog or standalone transaction or an unknown method, the P-CSCF based on local policy may include a P-Access-Network-Info header field. The value of the "dvb-rcs2-node-id" parameter shall be provided by the IP-CAN.

### S.3.3 Procedures at the S-CSCF

#### S.3.3.1 Notification of AS about registration status

Not applicable

---

### S.4 3GPP specific encoding for SIP header field extensions

Void.

---

### S.5 Use of circuit-switched domain

There is no CS domain in this access technology.

## Annex T (informative): Change history

| Change history |       |               |    |     |   |     |     |        |
|----------------|-------|---------------|----|-----|---|-----|-----|--------|
| Date           | TSG # | TSG Doc.      | CR | Rev | Subject/Comment   | Old | New | WG doc |
|                |       |               |    |     | Version 0.0.0 Editor's internal draft   |     |     |        |
|                |       |               |    |     | Version 0.0.1 Editor's internal draft   |     |     |        |
|                |       |               |    |     | Version 0.0.2 Editor's internal draft   |     |     |        |
|                |       | N1-001060     |    |     | Version 0.0.3 Submitted to CN1 SIP adhoc #1   |     |     |        |
| 19/10/00       |       | N1-001109     |    |     | Version 0.0.4 Reflecting results of initial CN1 discussion  |     |     |        |
| 19/10/00       |       | N1-001115     |    |     | Version 0.0.5 Reflecting output of CN1 SIP adhoc#1 discussion   |     |     |        |
| 09/11/00       |       |               |    |     | Version 0.0.6 Revision to include latest template and styles  |     |     |        |
|                |       | N1-010092     |    |     | Version 0.0.7 Reflecting updates of some IETF drafts  |     |     |        |
| 14/02/01       |       | N1-010269     |    |     | Version 0.0.8 Revision to include temporary annex B incorporating valuable source material  |     |     |        |
| 18/03/01       |       | N1-010378 rev |    |     | Version 0.1.0 incorporating results of CN1 discussion at CN1 #16  |     |     |        |
| 12/04/01       |       | N1-010737     |    |     | Version 0.2.0 incorporating results of CN1 discussions at SIP adhoc #4  |     |     |        |
| 11/06/01       |       | N1-010935     |    |     | Version 0.3.0 incorporating results of CN1 discussions at CN1 #16   |     |     |        |
| 23/07/01       |       | N1-011103     |    |     | Version 0.4.0 incorporating results of CN1 discussions at CN1 #18 (agreed documents N1-011028, N1-011050, N1-011055, N1-011056)   |     |     |        |
| 12/09/01       |       | N1-011385     |    |     | Version 0.5.0 incorporating results of CN1 discussions at CN1 #19 (agreed documents N1-011109, N1-011152, N1-011195, N1-011312, N1-011319, N1-011343)   |     |     |        |
| 04/10/01       |       | N1-011470     |    |     | Version 0.6.0 incorporating results of CN1 discussions at CN1 #19bis (agreed documents N1-011346, N1-011373, N1-011389, N1-011390, N1-011392, N1-011393, N1-011394, N1-011408, N1-011410, N1-011426)  |     |     |        |
| 19/10/01       |       | N1-011643     |    |     | Version 0.7.0 incorporating results of CN1 discussions at CN1 #20 (agreed documents N1-011477, N1-011479, N1-011498, N1-011523, N1-011548, N1-011585, N1-011586, N1-011592, N1-011611, N1-011629)   |     |     |        |
| 16/11/01       |       | N1-011821     |    |     | Version 0.8.0 incorporating results of CN1 discussions at CN1 #20bis (agreed documents N1-011685, N1-011690, N1-011741, N1-011743, N1-011759, N1-011760, N1-011761, N1-011765c, N1-011767, N1-011769, N1-011770, N1-011771, N1-011774, N1-011777, N1-011779, N1-011780) N1-011712 was agreed but determined to have no impact on the specification at this time.  |     |     |        |
| 30/11/01       |       | N1-020010     |    |     | Version 1.0.0 incorporating results of CN1 discussions at CN1 #21 (agreed documents N1-011828, N1-011829, N1-011836, N1-011899 [revision marks not used on moved text - additional change from chairman's report incorporated], implementation of subclause 3.1 editor's note based on discussion of N1-011900 [chairman's report], N1-011905, N1-011984, N1-011985, N1-011986, N1-011988, N1-011989, N1-012012 [excluding points 2 and 16], N1-012013, N1-012014 [excluding point 1], N1-012015, N1-012021, N1-012022, N1-012025, N1-012031, N1-012045, N1-012056, N1-012057) CN1 agreed for presentation for information to CN plenary. |     |     |        |
| 18/01/02       |       | N1-020189     |    |     | Version 1.1.0 incorporating results of CN1 discussions at CN1 SIP ad-hoc (agreed documents N1-020015, N1-020053, N1-020064, N1-020101, N1-020123, N1-020124, N1-020142, N1-020146, N1-020147, N1-020148, N1-020151, N1-020157, N1-020159, N1-020165). Also N1-012000 (agreed at previous meeting) required, subclause 5.2.6 to be deleted and this change has been enacted  |     |     |        |

| Change history |           |           |     |     |  |       |       |           |
|----------------|-----------|-----------|-----|-----|--|-------|-------|-----------|
| Date           | TSG #     | TSG Doc.  | CR  | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 01/02/02       |           | N1-020459 |     |     | Version 1.2.0 incorporating results of CN1 discussions at CN1 #22 (agreed documents N1-020198, N1-020396, N1-020398, N1-020399, N1-020408, N1-020417, N1-020418, N1-020419, N1-020421, N1-020422, N1-020436, N1-020437, N1-020449)   |       |       |           |
| 01/02/02       |           | N1-020569 |     |     | Version 1.2.1 issues to correct cut and paste error in incorporation of Annex B into main document. Affected subclause 5.1.1.3. Change to clause 7 title that was incorrectly applied to subclause 7.2 also corrected.   |       |       |           |
| 22/02/02       |           |           |     |     | Advanced to version 2.0.0 based on agreement of N1-020515.<br>Version 2.0.0 incorporating results of CN1 discussions at CN1 #22bis (agreed documents N1-020466, N1-020468, N1-020469, N1-020472, N1-020473, N1-020500, N1-020504, N1-020507, N1-020511, N1-020512, N1-020521, N1-020583, N1-020584, N1-020602, N1-020603, N1-020604, N1-020611, N1-020612, N1-020613, N1-020614, N1-020615, N1-020617, N1-020623, N1-020624, N1-020625, N1-020626, N1-020627, N1-020642, N1-020643, N1-020646, N1-020649, N1-020656, N1-020659, N1-020668, N1-020669, N1-020670, N1-020671).<br>In addition N1-020409, agreed at CN1#22 but missed from the previous version, was also implemented.<br>References have been resequenced. |       |       |           |
| 02/03/02       |           |           |     |     | Editorial clean-up by ETSI/MCC.  | 2.0.0 | 2.0.1 |           |
| 11/03/02       | TSG CN#15 | NP-020049 |     |     | The draft was approved, and 3GPP TS 24.229 was then to be issued in Rel-5 under formal change control.   | 2.0.1 | 5.0.0 |           |
| 2002-06        | NP-16     | NP-020230 | 004 | 1   | S-CSCF Actions on Authentication Failure   | 5.0.0 | 5.1.0 | N1-020903 |
| 2002-06        | NP-16     | NP-020230 | 005 | 2   | Disallow Parallel Registrations  | 5.0.0 | 5.1.0 | N1-020959 |
| 2002-06        | NP-16     | NP-020230 | 007 | 1   | Hiding   | 5.0.0 | 5.1.0 | N1-020910 |
| 2002-06        | NP-16     | NP-020312 | 008 | 8   | Support for services for unregistered users  | 5.0.0 | 5.1.0 |           |
| 2002-06        |           |           | 009 | 1   | Not implemented nor implementable. In the meeting report CN1#24 under doc N1-021513 it is shown that CR095r2 supercedes 009r1 if 095r2 was to be approved in CN#16 (but unfortunately 009r1 was also approved in the the CN#16 draft minutes).   |       |       | N1-020921 |
| 2002-06        | NP-16     | NP-020231 | 019 |     | MGCF procedure clarification   | 5.0.0 | 5.1.0 | N1-020788 |
| 2002-06        | NP-16     | NP-020231 | 020 | 2   | MGCF procedure error cases   | 5.0.0 | 5.1.0 | N1-020960 |
| 2002-06        | NP-16     | NP-020231 | 022 | 1   | Abbreviations clean up   | 5.0.0 | 5.1.0 | N1-020949 |
| 2002-06        | NP-16     | NP-020231 | 023 |     | Clarification of SIP usage outside IM CN subsystem   | 5.0.0 | 5.1.0 | N1-020792 |
| 2002-06        | NP-16     | NP-020314 | 024 | 3   | Replacement of COMET by UPDATE   | 5.0.0 | 5.1.0 |           |
| 2002-06        | NP-16     | NP-020231 | 025 | 3   | Incorporation of current RFC numbers   | 5.0.0 | 5.1.0 | N1-021091 |
| 2002-06        | NP-16     | NP-020231 | 026 | 1   | Clarification of B2BUA usage in roles  | 5.0.0 | 5.1.0 | N1-020941 |
| 2002-06        | NP-16     | NP-020231 | 028 | 4   | Determination of MO / MT requests in I-CSCF(THIG)  | 5.0.0 | 5.1.0 | N1-021248 |
| 2002-06        | NP-16     | NP-020231 | 030 | 2   | P-CSCF release of an existing session  | 5.0.0 | 5.1.0 | N1-021006 |
| 2002-06        | NP-16     | NP-020232 | 031 | 1   | S-CSCF release of an existing session  | 5.0.0 | 5.1.0 | N1-020939 |
| 2002-06        | NP-16     | NP-020232 | 033 | 3   | SDP procedure at the UE  | 5.0.0 | 5.1.0 | N1-020971 |
| 2002-06        | NP-16     | NP-020232 | 035 | 1   | AS Procedures corrections  | 5.0.0 | 5.1.0 | N1-020934 |
| 2002-06        | NP-16     | NP-020232 | 036 | 8   | Corrections to SIP Compression   | 5.0.0 | 5.1.0 | N1-021499 |

| Change history |       |           |     |     |   |       |       |           |
|----------------|-------|-----------|-----|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2002-06        | NP-16 | NP-020232 | 037 | 1   | Enhancement of S-CSCF and I-CSCF Routing Procedures for interworking with external networks   | 5.0.0 | 5.1.0 | N1-020928 |
| 2002-06        | NP-16 | NP-020232 | 041 | 2   | Delivery of IMS security parameters from S-CSCF to the P-CSCF by using proprietary auth-param | 5.0.0 | 5.1.0 | N1-021003 |
| 2002-06        | NP-16 | NP-020232 | 045 |     | Cleanup of request / response terminology - clause 5  | 5.0.0 | 5.1.0 | N1-020835 |
| 2002-06        | NP-16 | NP-020232 | 046 |     | Cleanup of request / response terminology - clause 6  | 5.0.0 | 5.1.0 | N1-020836 |
| 2002-06        | NP-16 | NP-020232 | 047 | 2   | Simplification of profile tables  | 5.0.0 | 5.1.0 | N1-021059 |
| 2002-06        | NP-16 | NP-020232 | 049 |     | Forking options   | 5.0.0 | 5.1.0 | N1-020839 |
| 2002-06        | NP-16 | NP-020315 | 050 | 1   | Media-Authorization header corrections  | 5.0.0 | 5.1.0 |           |
| 2002-06        | NP-16 | NP-020233 | 051 | 1   | Clause 5.4 editorials (S-CSCF)  | 5.0.0 | 5.1.0 | N1-020950 |
| 2002-06        | NP-16 | NP-020233 | 053 | 2   | Integrity protection signalling from the P-CSCF to the S-CSCF                                 | 5.0.0 | 5.1.0 | N1-021007 |
| 2002-06        | NP-16 | NP-020233 | 054 |     | Representing IM CN subsystem functional entities in profile table roles                       | 5.0.0 | 5.1.0 | N1-020847 |
| 2002-06        | NP-16 | NP-020233 | 055 |     | Clause 4 editorials   | 5.0.0 | 5.1.0 | N1-020848 |
| 2002-06        | NP-16 | NP-020233 | 056 |     | Clause 5.8 editorials (MRFC)  | 5.0.0 | 5.1.0 | N1-020849 |
| 2002-06        | NP-16 | NP-020233 | 057 | 1   | Annex A editorials, including precondition additions  | 5.0.0 | 5.1.0 | N1-021001 |
| 2002-06        | NP-16 | NP-020233 | 058 | 2   | Representing the registrar as a UA  | 5.0.0 | 5.1.0 | N1-021054 |
| 2002-06        | NP-16 | NP-020233 | 059 |     | Additional definitions  | 5.0.0 | 5.1.0 | N1-020852 |
| 2002-06        | NP-16 | NP-020312 | 060 | 11  | Restructuring of S-CSCF Registration Sections   | 5.0.0 | 5.1.0 |           |
| 2002-06        | NP-16 | NP-020234 | 061 | 2   | Determination of MOC / MTC at P-CSCF and S-CSCF   | 5.0.0 | 5.1.0 | N1-021060 |
| 2002-06        | NP-16 | NP-020234 | 062 |     | Correction to the terminating procedures  | 5.0.0 | 5.1.0 | N1-020927 |
| 2002-06        | NP-16 | NP-020234 | 063 |     | Loose Routing for Network Initiated Call Release Procedures                                   | 5.0.0 | 5.1.0 | N1-020940 |
| 2002-06        | NP-16 | NP-020234 | 064 |     | Incorporation of previously agreed corrections to clause 5.2.5.2 (N1-020416)                  | 5.0.0 | 5.1.0 | N1-021004 |
| 2002-06        | NP-16 | NP-020234 | 065 |     | Clause 7.2 editorial corrections  | 5.0.0 | 5.1.0 | N1-021005 |
| 2002-06        | NP-16 | NP-020234 | 067 | 2   | S-CSCF routing of MO calls  | 5.0.0 | 5.1.0 | N1-021097 |
| 2002-06        | NP-16 | NP-020234 | 068 | 1   | I-CSCF routing of dialog requests   | 5.0.0 | 5.1.0 | N1-021078 |
| 2002-06        | NP-16 | NP-020234 | 069 | 2   | Definition of the Tokenised-by parameter  | 5.0.0 | 5.1.0 | N1-021096 |
| 2002-06        | NP-16 | NP-020235 | 070 | 3   | SDP procedures at UE  | 5.0.0 | 5.1.0 | N1-021453 |
| 2002-06        | NP-16 | NP-020235 | 073 | 2   | Updates to the procedures involving the iFCs, following the Oulu iFC changes                  | 5.0.0 | 5.1.0 | N1-021440 |
| 2002-06        | NP-16 | NP-020235 | 074 | 1   | Addition of DHCPv6 references to 24.229   | 5.0.0 | 5.1.0 | N1-021086 |
| 2002-06        | NP-16 | NP-020235 | 075 | 1   | Clarification to URL and address assignments  | 5.0.0 | 5.1.0 | N1-021083 |
| 2002-06        | NP-16 | NP-020235 | 079 | 3   | Downloading the implicitly registered public user identities from the S-CSCF to P-CSCF        | 5.0.0 | 5.1.0 | N1-021510 |
| 2002-06        | NP-16 | NP-020235 | 080 | 3   | Clarification of GPRS aspects   | 5.0.0 | 5.1.0 | N1-021486 |
| 2002-06        | NP-16 | NP-020235 | 081 | 2   | Introduction of Subscription Locator Function Interrogation at I-CSCF in 24.229               | 5.0.0 | 5.1.0 | N1-021469 |
| 2002-06        | NP-16 | NP-020235 | 082 | 1   | Introduction of Visited_Network_ID p-header   | 5.0.0 | 5.1.0 | N1-021433 |
| 2002-06        | NP-16 | NP-020236 | 084 | 1   | MRFC register addresses   | 5.0.0 | 5.1.0 | N1-021434 |
| 2002-06        | NP-16 | NP-020236 | 085 | 1   | MRFC INVITE interface editor's notes  | 5.0.0 | 5.1.0 | N1-021470 |
| 2002-06        | NP-16 | NP-020236 | 086 | 1   | MRFC OPTIONS interface editor's notes   | 5.0.0 | 5.1.0 | N1-021471 |
| 2002-06        | NP-16 | NP-020236 | 087 |     | MRFC PRACK & INFO editor's notes  | 5.0.0 | 5.1.0 | N1-021159 |



| Change history |       |           |     |     |  |       |       |           |
|----------------|-------|-----------|-----|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2002-06        | NP-16 | NP-020236 | 088 | 1   | MGCF OPTIONS interface editor's notes                              | 5.0.0 | 5.1.0 | N1-021472 |
| 2002-06        | NP-16 | NP-020236 | 089 |     | MGCF reINVITE editor's notes                                       | 5.0.0 | 5.1.0 | N1-021161 |
| 2002-06        | NP-16 | NP-020237 | 090 |     | 3PCC AS editor's notes   | 5.0.0 | 5.1.0 | N1-021162 |
| 2002-06        | NP-16 | NP-020237 | 091 |     | AS acting as terminating UA editor's notes                         | 5.0.0 | 5.1.0 | N1-021163 |
| 2002-06        | NP-16 | NP-020237 | 092 | 1   | AS acting as originating UA editor's notes                         | 5.0.0 | 5.1.0 | N1-021466 |
| 2002-06        | NP-16 | NP-020237 | 093 | 2   | Charging overview clause   | 5.0.0 | 5.1.0 | N1-021512 |
| 2002-06        | NP-16 | NP-020237 | 094 | 1   | Procedures for original-dialog-id P-header                         | 5.0.0 | 5.1.0 | N1-021456 |
| 2002-06        | NP-16 | NP-020237 | 095 | 2   | Procedures for charging-vector P-header                            | 5.0.0 | 5.1.0 | N1-021513 |
| 2002-06        | NP-16 | NP-020237 | 096 | 1   | Procedures for charging-function-addresses P-header                | 5.0.0 | 5.1.0 | N1-021458 |
| 2002-06        | NP-16 | NP-020237 | 097 | 1   | SDP types  | 5.0.0 | 5.1.0 | N1-021467 |
| 2002-06        | NP-16 | NP-020237 | 100 |     | Removal of State from profile tables                               | 5.0.0 | 5.1.0 | N1-021173 |
| 2002-06        | NP-16 | NP-020238 | 101 |     | Editor's note cleanup - clause 3                                   | 5.0.0 | 5.1.0 | N1-021174 |
| 2002-06        | NP-16 | NP-020238 | 102 |     | Editor's note cleanup - clause 4                                   | 5.0.0 | 5.1.0 | N1-021175 |
| 2002-06        | NP-16 | NP-020238 | 103 |     | Editor's note cleanup - clause 5.1 and deletion of void subclauses | 5.0.0 | 5.1.0 | N1-021176 |
| 2002-06        | NP-16 | NP-020238 | 104 | 1   | Editor's note cleanup - clause 5.2 and deletion of void subclauses | 5.0.0 | 5.1.0 | N1-021487 |
| 2002-06        | NP-16 | NP-020238 | 105 |     | Editor's note cleanup - clause 5.3                                 | 5.0.0 | 5.1.0 | N1-021178 |
| 2002-06        | NP-16 | NP-020238 | 106 |     | Editor's note cleanup - clause 5.4 and deletion of void subclauses | 5.0.0 | 5.1.0 | N1-021179 |
| 2002-06        | NP-16 | NP-020238 | 107 |     | Editor's note cleanup - clause 5.5 and deletion of void subclauses | 5.0.0 | 5.1.0 | N1-021180 |
| 2002-06        | NP-16 | NP-020238 | 110 |     | Editor's note cleanup - clause 6                                   | 5.0.0 | 5.1.0 | N1-021183 |
| 2002-06        | NP-16 | NP-020238 | 111 |     | Editor's note cleanup - clause 9                                   | 5.0.0 | 5.1.0 | N1-021184 |
| 2002-06        | NP-16 | NP-020239 | 113 | 1   | SIP Default Timers   | 5.0.0 | 5.1.0 | N1-021465 |
| 2002-06        | NP-16 | NP-020239 | 114 | 1   | Correction of the subscription to the registration event package   | 5.0.0 | 5.1.0 | N1-021436 |
| 2002-06        | NP-16 | NP-020239 | 115 | 1   | Support for ISIMless UICC  | 5.0.0 | 5.1.0 | N1-021441 |
| 2002-06        | NP-16 | NP-020239 | 119 | 1   | SIP procedures at UE   | 5.0.0 | 5.1.0 | N1-021452 |
| 2002-06        | NP-16 | NP-020239 | 121 | 2   | New requirements in the P-CSCF                                     | 5.0.0 | 5.1.0 | N1-021509 |
| 2002-06        | NP-16 | NP-020239 | 122 |     | SDP procedures at MGCF   | 5.0.0 | 5.1.0 | N1-021264 |
| 2002-06        | NP-16 | NP-020239 | 124 | 1   | S-CSCF allocation  | 5.0.0 | 5.1.0 | N1-021443 |
| 2002-06        | NP-16 | NP-020240 | 129 | 1   | Introduction of P-Access-Network-Info header                       | 5.0.0 | 5.1.0 | N1-021498 |
| 2002-06        | NP-16 | NP-020240 | 130 | 2   | Usage of Path and P-Service Route                                  | 5.0.0 | 5.1.0 | N1-021508 |
| 2002-06        | NP-16 | NP-020240 | 133 |     | Removal of Referred-By header from specification                   | 5.0.0 | 5.1.0 | N1-021354 |
| 2002-06        | NP-16 | NP-020240 | 134 |     | Handling of Record-Route header in profile tables                  | 5.0.0 | 5.1.0 | N1-021357 |
| 2002-06        | NP-16 | NP-020312 | 135 | 1   | Asserted identities and privacy                                    | 5.0.0 | 5.1.0 |           |
| 2002-06        | NP-16 | NP-020240 | 136 |     | Removal of caller preferences from specification                   | 5.0.0 | 5.1.0 | N1-021359 |
| 2002-06        | NP-16 | NP-020240 | 137 |     | Substitution of REFER references                                   | 5.0.0 | 5.1.0 | N1-021360 |
| 2002-06        | NP-16 | NP-020240 | 138 |     | Removal of session timer from specification                        | 5.0.0 | 5.1.0 | N1-021361 |
| 2002-09        | NP-17 | NP-020489 | 141 | 2   | Adding MESSAGE to 24.229   | 5.1.0 | 5.2.0 |           |

| Change history |       |           |     |     |  |       |       |           |
|----------------|-------|-----------|-----|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2002-09        | NP-17 | NP-020375 | 142 |     | Public user identity to use for third party register                 | 5.1.0 | 5.2.0 | N1-021563 |
| 2002-09        | NP-17 | NP-020375 | 143 | 1   | Replace P-Original-Dialog-ID header with unique data in Route header | 5.1.0 | 5.2.0 | N1-021797 |
| 2002-09        | NP-17 | NP-020375 | 145 |     | Synchronize text with latest I-D for P-headers for charging          | 5.1.0 | 5.2.0 | N1-021569 |
| 2002-09        | NP-17 | NP-020488 | 146 | 2   | Service profiles and implicitly registered public user identities    | 5.1.0 | 5.2.0 |           |
| 2002-09        | NP-17 | NP-020376 | 147 |     | S-CSCF decides when to include                                       | 5.1.0 | 5.2.0 | N1-021571 |
| 2002-09        | NP-17 | NP-020376 | 148 |     | Clean up XML in clause 7.6   | 5.1.0 | 5.2.0 | N1-021572 |
| 2002-09        | NP-17 | NP-020376 | 149 |     | Fix clause 5.2.7.4 header  | 5.1.0 | 5.2.0 | N1-021573 |
| 2002-09        | NP-17 | NP-020376 | 150 |     | Removal of forward reference to non P-CSCF procedures                | 5.1.0 | 5.2.0 | N1-021589 |
| 2002-09        | NP-17 | NP-020376 | 151 |     | Deregistration of public user identities                             | 5.1.0 | 5.2.0 | N1-021590 |
| 2002-09        | NP-17 | NP-020376 | 152 |     | Reauthentication trigger via other means                             | 5.1.0 | 5.2.0 | N1-021591 |
| 2002-09        | NP-17 | NP-020487 | 153 | 3   | Registration with integrity protection                               | 5.1.0 | 5.2.0 |           |
| 2002-09        | NP-17 | NP-020485 | 154 | 2   | Explicit listing of need to route response messages                  | 5.1.0 | 5.2.0 |           |
| 2002-09        | NP-17 | NP-020377 | 157 | 1   | Include IP address in ICID   | 5.1.0 | 5.2.0 | N1-021816 |
| 2002-09        | NP-17 | NP-020377 | 158 |     | Reference updates  | 5.1.0 | 5.2.0 | N1-021604 |
| 2002-09        | NP-17 | NP-020377 | 159 |     | Abbreviation updates   | 5.1.0 | 5.2.0 | N1-021605 |
| 2002-09        | NP-17 | NP-020377 | 163 | 1   | Clarifications of allocation of IP address                           | 5.1.0 | 5.2.0 | N1-021817 |
| 2002-09        | NP-17 | NP-020377 | 171 | 1   | Verifications at the P-CSCF for subsequent request                   | 5.1.0 | 5.2.0 | N1-021802 |
| 2002-09        | NP-17 | NP-020377 | 174 | 1   | Clarification of IMS signalling flag                                 | 5.1.0 | 5.2.0 | N1-021781 |
| 2002-09        | NP-17 | NP-020377 | 176 | 1   | Definition of a general-purpose PDP context for IMS                  | 5.1.0 | 5.2.0 | N1-021783 |
| 2002-09        | NP-17 | NP-020372 | 177 | 2   | Request for DNS IPv6 server address                                  | 5.1.0 | 5.2.0 | N1-021833 |
| 2002-09        | NP-17 | NP-020378 | 178 |     | Error cases for PDP context modification                             | 5.1.0 | 5.2.0 | N1-021679 |
| 2002-09        | NP-17 | NP-020378 | 183 | 1   | Incorporation of draft-ietf-sip-sec-agree-04.txt                     | 5.1.0 | 5.2.0 | N1-021791 |
| 2002-09        | NP-17 | NP-020378 | 185 | 1   | User Initiated De-registration                                       | 5.1.0 | 5.2.0 | N1-021787 |
| 2002-09        | NP-17 | NP-020378 | 186 | 1   | Mobile initiated de-registration                                     | 5.1.0 | 5.2.0 | N1-021788 |
| 2002-09        | NP-17 | NP-020378 | 187 | 1   | CallID of REGISTER requests  | 5.1.0 | 5.2.0 | N1-021786 |
| 2002-09        | NP-17 | NP-020378 | 188 | 1   | Correction to the I-CSCF routing procedures                          | 5.1.0 | 5.2.0 | N1-021803 |
| 2002-09        | NP-17 | NP-020378 | 189 | 1   | Registration procedures at P-CSCF                                    | 5.1.0 | 5.2.0 | N1-021793 |
| 2002-09        | NP-17 | NP-020378 | 192 | 1   | Corrections related to the P-Access-Network-Info header              | 5.1.0 | 5.2.0 | N1-021827 |
| 2002-09        | NP-17 | NP-020378 | 194 | 1   | Chapter to describe the registration event                           | 5.1.0 | 5.2.0 | N1-021794 |
| 2002-09        | NP-17 | NP-020484 | 196 |     | Definition of abbreviation IMS                                       | 5.1.0 | 5.2.0 |           |
| 2002-12        | NP-18 | NP-020558 | 140 | 4   | Support of non-IMS forking   | 5.2.0 | 5.3.0 | N1-022446 |
| 2002-12        | NP-18 | NP-020565 | 144 | 2   | Identification of supported IETF drafts within this release          | 5.2.0 | 5.3.0 | N1-022114 |
| 2002-12        | NP-18 | NP-020558 | 161 | 3   | Clarifications and editorials to SIP profile                         | 5.2.0 | 5.3.0 | N1-022412 |
| 2002-12        | NP-18 | NP-020558 | 175 | 5   | Clarifications of the binding and media grouping                     | 5.2.0 | 5.3.0 | N1-022494 |
| 2002-12        | NP-18 | NP-020558 | 179 | 2   | Support of originating requests from Application Servers             | 5.2.0 | 5.3.0 | N1-022106 |

| Change history |       |           |     |     |  |       |       |           |
|----------------|-------|-----------|-----|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2002-12        | NP-18 | NP-020558 | 197 |     | Wrong references in 4.1  | 5.2.0 | 5.3.0 | N1-021902 |
| 2002-12        | NP-18 | NP-020558 | 198 |     | Alignment of the MGCF procedures to RFC 3312   | 5.2.0 | 5.3.0 | N1-021903 |
| 2002-12        | NP-18 | NP-020558 | 199 | 1   | Service Route Header and Path Header interactions                                    | 5.2.0 | 5.3.0 | N1-022080 |
| 2002-12        | NP-18 | NP-020558 | 202 |     | Addition of clause 6 though clause 9 references to conformance clause                | 5.2.0 | 5.3.0 | N1-021919 |
| 2002-12        | NP-18 | NP-020558 | 203 | 1   | URL and address assignments  | 5.2.0 | 5.3.0 | N1-022115 |
| 2002-12        | NP-18 | NP-020559 | 204 | 3   | Fix gprs-charging-info definition and descriptions                                   | 5.2.0 | 5.3.0 | N1-022426 |
| 2002-12        | NP-18 | NP-020559 | 206 |     | Alignment of the SDP attributes related to QoS integration with IETF                 | 5.2.0 | 5.3.0 | N1-021930 |
| 2002-12        | NP-18 | NP-020559 | 207 | 1   | Update of the 3GPP-generated SIP P- headers document references                      | 5.2.0 | 5.3.0 | N1-022116 |
| 2002-12        | NP-18 | NP-020559 | 208 | 1   | Handling of INVITE requests that do not contain SDP                                  | 5.2.0 | 5.3.0 | N1-022098 |
| 2002-12        | NP-18 | NP-020559 | 209 | 2   | UE Registration  | 5.2.0 | 5.3.0 | N1-022471 |
| 2002-12        | NP-18 | NP-020559 | 211 | 1   | Usage of private user identity during registration                                   | 5.2.0 | 5.3.0 | N1-022083 |
| 2002-12        | NP-18 | NP-020559 | 212 | 1   | P-CSCF subscription to the users registration-state event                            | 5.2.0 | 5.3.0 | N1-022084 |
| 2002-12        | NP-18 | NP-020559 | 213 | 2   | Handling of MT call by the P-CSCF  | 5.2.0 | 5.3.0 | N1-022154 |
| 2002-12        | NP-18 | NP-020559 | 215 |     | P-CSCF acting as a UA  | 5.2.0 | 5.3.0 | N1-021939 |
| 2002-12        | NP-18 | NP-020559 | 216 | 1   | S-CSCF handling of protected registrations   | 5.2.0 | 5.3.0 | N1-022085 |
| 2002-12        | NP-18 | NP-020560 | 217 | 1   | S-CSCF handling of subscription to the users registration-state event                | 5.2.0 | 5.3.0 | N1-022086 |
| 2002-12        | NP-18 | NP-020560 | 218 | 1   | Determination of MO or MT in I-CSCF  | 5.2.0 | 5.3.0 | N1-022102 |
| 2002-12        | NP-18 | NP-020560 | 220 |     | Definition of the NAI and RTCP abbreviations   | 5.2.0 | 5.3.0 | N1-021944 |
| 2002-12        | NP-18 | NP-020560 | 222 | 4   | Go related error codes in the UE   | 5.2.0 | 5.3.0 | N1-022495 |
| 2002-12        | NP-18 | NP-020560 | 223 | 1   | Clarifications on CCF/ECF addresses  | 5.2.0 | 5.3.0 | N1-022120 |
| 2002-12        | NP-18 | NP-020560 | 225 | 2   | Clarifications on dedicated PDP Context for IMS signalling                           | 5.2.0 | 5.3.0 | N1-022156 |
| 2002-12        | NP-18 | NP-020560 | 228 | 3   | Clarifications on the use of charging correlation information                        | 5.2.0 | 5.3.0 | N1-022425 |
| 2002-12        | NP-18 | NP-020560 | 232 | 1   | Expires information in REGISTER response   | 5.2.0 | 5.3.0 | N1-022095 |
| 2002-12        | NP-18 | NP-020560 | 235 | 2   | Indication of successful establishment of Dedicated Signalling PDP context to the UE | 5.2.0 | 5.3.0 | N1-022129 |
| 2002-12        | NP-18 | NP-020560 | 237 |     | P-CSCF sending 100 (Trying) Response for reINVITE                                    | 5.2.0 | 5.3.0 | N1-021998 |
| 2002-12        | NP-18 | NP-020561 | 239 | 1   | Correction on P-Asserted-Id, P-Preferred-Id, Remote-Party-ID                         | 5.2.0 | 5.3.0 | N1-022100 |
| 2002-12        | NP-18 | NP-020561 | 240 | 1   | Clarifications to subclause 9.2.5  | 5.2.0 | 5.3.0 | N1-022137 |
| 2002-12        | NP-18 | NP-020561 | 242 |     | ENUM translation   | 5.2.0 | 5.3.0 | N1-022020 |
| 2002-12        | NP-18 | NP-020561 | 243 | 1   | AS routing   | 5.2.0 | 5.3.0 | N1-022107 |
| 2002-12        | NP-18 | NP-020561 | 245 | 1   | Warning header   | 5.2.0 | 5.3.0 | N1-022108 |

| Change history |       |           |     |     |  |       |       |           |
|----------------|-------|-----------|-----|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2002-12        | NP-18 | NP-020561 | 246 | 3   | S-CSCF procedure tidyup  | 5.2.0 | 5.3.0 | N1-022497 |
| 2002-12        | NP-18 | NP-020561 | 247 | 1   | P-CSCF procedure tidyup  | 5.2.0 | 5.3.0 | N1-022125 |
| 2002-12        | NP-18 | NP-020561 | 248 | 2   | UE procedure tidyup  | 5.2.0 | 5.3.0 | N1-022472 |
| 2002-12        | NP-18 | NP-020561 | 249 | 3   | MESSAGE corrections part 1   | 5.2.0 | 5.3.0 | N1-022455 |
| 2002-12        | NP-18 | NP-020561 | 250 | 2   | MESSAGE corrections part 2   | 5.2.0 | 5.3.0 | N1-022456 |
| 2002-12        | NP-18 | NP-020562 | 251 | 2   | Security association clarifications  | 5.2.0 | 5.3.0 | N1-022440 |
| 2002-12        | NP-18 | NP-020562 | 252 | 1   | The use of security association by the UE  | 5.2.0 | 5.3.0 | N1-022433 |
| 2002-12        | NP-18 | NP-020562 | 253 | 1   | UE integrity protected re-registration   | 5.2.0 | 5.3.0 | N1-022434 |
| 2002-12        | NP-18 | NP-020562 | 255 | 3   | Handling of default public user identities by the P-CSCF   | 5.2.0 | 5.3.0 | N1-022496 |
| 2002-12        | NP-18 | NP-020562 | 263 |     | Fixing ioi descriptions  | 5.2.0 | 5.3.0 | N1-022266 |
| 2002-12        | NP-18 | NP-020562 | 264 | 1   | Fix descriptions for ECF/CCF addresses   | 5.2.0 | 5.3.0 | N1-022447 |
| 2002-12        | NP-18 | NP-020562 | 266 | 2   | Alignment with draft-ietf-sipping-reg-event-00 and clarification on network initiated deregistration | 5.2.0 | 5.3.0 | N1-022493 |
| 2002-12        | NP-18 | NP-020563 | 267 | 1   | Correction to network initiated re-authentication procedure  | 5.2.0 | 5.3.0 | N1-022449 |
| 2002-12        | NP-18 | NP-020563 | 268 | 1   | Registration Expires Timer Default Setting   | 5.2.0 | 5.3.0 | N1-022439 |
| 2002-12        | NP-18 | NP-020563 | 269 | 1   | Clarification on Sh interface for charging purposes  | 5.2.0 | 5.3.0 | N1-022465 |
| 2002-12        | NP-18 | NP-020563 | 270 | 2   | Clarifications on the scope  | 5.2.0 | 5.3.0 | N1-022500 |
| 2002-12        | NP-18 | NP-020563 | 273 | 1   | Add charging info for SUBSCRIBE  | 5.2.0 | 5.3.0 | N1-022467 |
| 2002-12        | NP-18 | NP-020563 | 274 | 1   | Profile revisions for RFC 3261 headers   | 5.2.0 | 5.3.0 | N1-022413 |
| 2002-12        | NP-18 | NP-020563 | 275 |     | Consistency changes for SDP procedures at MGCF   | 5.2.0 | 5.3.0 | N1-022345 |
| 2002-12        | NP-18 | NP-020563 | 276 |     | Proxy support of PRACK   | 5.2.0 | 5.3.0 | N1-022350 |
| 2002-12        | NP-18 | NP-020563 | 277 |     | Clarification of transparent handling of parameters in profile                                       | 5.2.0 | 5.3.0 | N1-022351 |
| 2002-12        | NP-18 | NP-020564 | 279 | 1   | Meaning of refresh request   | 5.2.0 | 5.3.0 | N1-022444 |
| 2002-12        | NP-18 | NP-020564 | 280 |     | Removal of Caller Preferences dependency   | 5.2.0 | 5.3.0 | N1-022362 |
| 2002-12        | NP-18 | NP-020564 | 281 | 1   | P-Access-Network-Info clarifications   | 5.2.0 | 5.3.0 | N1-022445 |
| 2002-12        | NP-18 | NP-020564 | 282 |     | Clarification on use of the From header by the UE  | 5.2.0 | 5.3.0 | N1-022370 |
| 2002-12        | NP-18 | NP-020634 | 283 | 2   | Support of comp=sigcomp parameter  | 5.2.0 | 5.3.0 |           |
| 2002-12        | NP-18 | NP-020668 | 284 | 4   | SDP media policy rejection   | 5.2.0 | 5.3.0 |           |
| 2002-12        | NP-18 | NP-020567 | 285 | 1   | Fallback for compression failure   | 5.2.0 | 5.3.0 | N1-022481 |
| 2002-12        | NP-18 | NP-020564 | 287 | 1   | SA related procedures  | 5.2.0 | 5.3.0 | N1-022459 |
| 2002-12        | NP-18 | NP-020568 | 290 | 1   | Emergency Service correction   | 5.2.0 | 5.3.0 | N1-022461 |
| 2002-12        | NP-18 | NP-020663 | 278 | 4   | P-CSCF does not strip away headers   | 5.2.0 | 5.3.0 | N1-022499 |
| 2002-12        | NP-18 | NP-020557 | 289 |     | PCF to PDF   | 5.2.0 | 5.3.0 | N1-022387 |
| 2003-03        | NP-19 | NP-030049 | 291 |     | Minor correction and consistency changes to general part of profile                                  | 5.3.0 | 5.4.0 | N1-030012 |

| Change history |       |           |     |     |  |       |       |           |
|----------------|-------|-----------|-----|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2003-03        | NP-19 | NP-030049 | 292 |     | SIP profile minor correction and consistency changes                         | 5.3.0 | 5.4.0 | N1-030013 |
| 2003-03        | NP-19 | NP-030049 | 293 | 1   | Network asserted identity procedure corrections for the UE                   | 5.3.0 | 5.4.0 | N1-030261 |
| 2003-03        | NP-19 | NP-030049 | 294 | 1   | Asserted identity inclusion in SIP profile                                   | 5.3.0 | 5.4.0 | N1-030300 |
| 2003-03        | NP-19 | NP-030049 | 296 |     | Profile references relating to registration                                  | 5.3.0 | 5.4.0 | N1-030023 |
| 2003-03        | NP-19 | NP-030049 | 297 | 2   | Reference corrections  | 5.3.0 | 5.4.0 | N1-030301 |
| 2003-03        | NP-19 | NP-030050 | 300 | 1   | 488 message with a subset of allowed media parameters                        | 5.3.0 | 5.4.0 | N1-030245 |
| 2003-03        | NP-19 | NP-030050 | 301 | 1   | Handling of Emergency Numbers in P-CSCF                                      | 5.3.0 | 5.4.0 | N1-030239 |
| 2003-03        | NP-19 | NP-030050 | 302 | 2   | Correction of the registration state event package                           | 5.3.0 | 5.4.0 | N1-030268 |
| 2003-03        | NP-19 | NP-030050 | 305 | 2   | User initiated de-registration at P-CSCF                                     | 5.3.0 | 5.4.0 | N1-030295 |
| 2003-03        | NP-19 | NP-030050 | 306 | 2   | Network-initiated deregistration at UE, P-CSCF, and S-CSCF                   | 5.3.0 | 5.4.0 | N1-030296 |
| 2003-03        | NP-19 | NP-030050 | 307 | 2   | UE deregistration during established dialogs                                 | 5.3.0 | 5.4.0 | N1-030297 |
| 2003-03        | NP-19 | NP-030050 | 308 | 2   | S-CSCF handling of deregistration during established dialogs                 | 5.3.0 | 5.4.0 | N1-030298 |
| 2003-03        | NP-19 | NP-030050 | 309 | 1   | S-CSCF handling of established dialogs upon deregistration                   | 5.3.0 | 5.4.0 | N1-030233 |
| 2003-03        | NP-19 | NP-030050 | 310 | 2   | S-CSCF handling of established dialogs upon registration-lifetime expiration | 5.3.0 | 5.4.0 | N1-030299 |
| 2003-03        | NP-19 | NP-030051 | 311 | 1   | P-CSCF handling of established dialogs upon registration-lifetime expiration | 5.3.0 | 5.4.0 | N1-030235 |
| 2003-03        | NP-19 | NP-030051 | 312 | 1   | Correction of Authentication procedure                                       | 5.3.0 | 5.4.0 | N1-030240 |
| 2003-03        | NP-19 | NP-030051 | 313 |     | Mixed Path header and Service-Route operation                                | 5.3.0 | 5.4.0 | N1-030127 |
| 2003-03        | NP-19 | NP-030051 | 315 | 2   | Clarifications on updating the authorization token                           | 5.3.0 | 5.4.0 | N1-030255 |
| 2003-03        | NP-19 | NP-030051 | 318 | 2   | Consideration of P-CSCF/PDF  | 5.3.0 | 5.4.0 | N1-030307 |
| 2003-03        | NP-19 | NP-030051 | 319 | 2   | Clarification on GPRS charging information                                   | 5.3.0 | 5.4.0 | N1-030308 |
| 2003-03        | NP-19 | NP-030051 | 323 | 1   | P-Access-Network-Info procedure corrections for the UE                       | 5.3.0 | 5.4.0 | N1-030250 |
| 2003-03        | NP-19 | NP-030051 | 324 | 1   | P-Access-Network-Info procedure corrections for the S-CSCF                   | 5.3.0 | 5.4.0 | N1-030251 |
| 2003-03        | NP-19 | NP-030051 | 326 | 1   | Updating user agent related profile tables                                   | 5.3.0 | 5.4.0 | N1-030260 |
| 2003-03        | NP-19 | NP-030052 | 327 | 2   | Cleanup and clarification to the registration and authentication procedure   | 5.3.0 | 5.4.0 | N1-030282 |
| 2003-03        | NP-19 | NP-030052 | 328 | 1   | Corrections to the reg event package   | 5.3.0 | 5.4.0 | N1-030230 |
| 2003-03        | NP-19 | NP-030052 | 330 | 2   | Clarifications for setting up separate PDP contexts in case of SBLP          | 5.3.0 | 5.4.0 | N1-030288 |
| 2003-03        | NP-19 | NP-030052 | 331 | 2   | Handling of the P-Media-Authorization header                                 | 5.3.0 | 5.4.0 | N1-030289 |
| 2003-03        | NP-19 | NP-030052 | 333 | 3   | Removal of P-Asserted-Identity from clause 7 of 24.229                       | 5.3.0 | 5.4.0 | N1-030310 |
| 2003-03        | NP-19 | NP-030052 | 334 |     | P-CSCF general procedure corrections   | 5.3.0 | 5.4.0 | N1-030182 |
| 2003-03        | NP-19 | NP-030052 | 335 | 2   | Usage of Contact in UE's registration procedure                              | 5.3.0 | 5.4.0 | N1-030281 |

| Change history |       |           |     |     |  |       |       |           |
|----------------|-------|-----------|-----|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2003-03        | NP-19 | NP-030052 | 337 |     | Usage of P-Asserted-Identity for responses   | 5.3.0 | 5.4.0 | N1-030193 |
| 2003-03        | NP-19 | NP-030052 | 339 | 2   | Authorization for registration event package   | 5.3.0 | 5.4.0 | N1-030285 |
| 2003-03        | NP-19 | NP-030052 | 341 | 1   | P-CSCF subscription to reg event   | 5.3.0 | 5.4.0 | N1-030284 |
| 2003-06        | NP-20 | NP-030275 | 295 | 4   | Security agreement inclusion in SIP profile  | 5.4.0 | 5.5.0 | N1-030939 |
| 2003-06        | NP-20 | NP-030275 | 322 | 5   | 3GPP P-header inclusion in SIP profile   | 5.4.0 | 5.5.0 | N1-030938 |
| 2003-06        | NP-20 | NP-030275 | 332 | 5   | Change of IP address for the UE  | 5.4.0 | 5.5.0 | N1-030923 |
| 2003-06        | NP-20 | NP-030275 | 342 |     | Removal of the requirement for UE re-authentication initiated by HSS                           | 5.4.0 | 5.5.0 | N1-030349 |
| 2003-06        | NP-20 | NP-030275 | 343 | 2   | UE behaviour on reception of 420 (Bad Extension) message                                       | 5.4.0 | 5.5.0 | N1-030552 |
| 2003-06        | NP-20 | NP-030275 | 347 | 2   | Handling of DTMF   | 5.4.0 | 5.5.0 | N1-030551 |
| 2003-06        | NP-20 | NP-030276 | 348 | 1   | Format of Tel URL in P-Asserted-Id   | 5.4.0 | 5.5.0 | N1-030510 |
| 2003-06        | NP-20 | NP-030276 | 349 |     | Delete Note on header stripping/SDP manipulation   | 5.4.0 | 5.5.0 | N1-030387 |
| 2003-06        | NP-20 | NP-030276 | 354 | 1   | Clarifications on using DNS procedures   | 5.4.0 | 5.5.0 | N1-030520 |
| 2003-06        | NP-20 | NP-030276 | 356 | 4   | Addition of procedures at the AS for SDP   | 5.4.0 | 5.5.0 | N1-030942 |
| 2003-06        | NP-20 | NP-030276 | 357 | 1   | Usage of P-Associated-URI  | 5.4.0 | 5.5.0 | N1-030499 |
| 2003-06        | NP-20 | NP-030276 | 359 | 1   | Network-initiated deregistration at UE and P-CSCF  | 5.4.0 | 5.5.0 | N1-030501 |
| 2003-06        | NP-20 | NP-030276 | 360 | 2   | Barred identities  | 5.4.0 | 5.5.0 | N1-030550 |
| 2003-06        | NP-20 | NP-030276 | 365 | 1   | PDP context subject to SBLP cannot be reused by other IMS sessions                             | 5.4.0 | 5.5.0 | N1-030513 |
| 2003-06        | NP-20 | NP-030276 | 368 | 1   | User authentication failure cleanups   | 5.4.0 | 5.5.0 | N1-030506 |
| 2003-06        | NP-20 | NP-030277 | 369 | 3   | S-CSCF behavior correction to enable call forwarding   | 5.4.0 | 5.5.0 | N1-030931 |
| 2003-06        | NP-20 | NP-030277 | 370 | 1   | SUBSCRIBE request information stored at the P-CSCF and S-CSCF                                  | 5.4.0 | 5.5.0 | N1-030521 |
| 2003-06        | NP-20 | NP-030277 | 371 | 1   | Profile Tables - Transparency  | 5.4.0 | 5.5.0 | N1-030858 |
| 2003-06        | NP-20 | NP-030277 | 375 | 1   | Profile Tables - Major Capability Corrections  | 5.4.0 | 5.5.0 | N1-030860 |
| 2003-06        | NP-20 | NP-030277 | 376 | 2   | Profile Tables - Deletion of Elements not used in 24.229                                       | 5.4.0 | 5.5.0 | N1-030921 |
| 2003-06        | NP-20 | NP-030277 | 377 | 1   | Use of the QoS parameter 'signalling information' for a signalling PDP context                 | 5.4.0 | 5.5.0 | N1-030840 |
| 2003-06        | NP-20 | NP-030277 | 378 | 2   | Deregistration of a PUID (not the last one)  | 5.4.0 | 5.5.0 | N1-030919 |
| 2003-06        | NP-20 | NP-030277 | 379 | 2   | 'Last registered public user identity' terminology change                                      | 5.4.0 | 5.5.0 | N1-030920 |
| 2003-06        | NP-20 | NP-030277 | 380 | 1   | Check Integrity Protection for P-Access-Network-Info header                                    | 5.4.0 | 5.5.0 | N1-030881 |
| 2003-06        | NP-20 | NP-030278 | 381 | 1   | PCSCF setting of Integrity protection indicator and checking of Security Verify header         | 5.4.0 | 5.5.0 | N1-030882 |
| 2003-06        | NP-20 | NP-030278 | 383 | 1   | Consistent treatment of register and de-register   | 5.4.0 | 5.5.0 | N1-030884 |
| 2003-06        | NP-20 | NP-030278 | 384 | 1   | Optionality of sending CK is removed   | 5.4.0 | 5.5.0 | N1-030885 |
| 2003-06        | NP-20 | NP-030278 | 385 | 1   | Addition of note and Correction of References regarding security associations and registration | 5.4.0 | 5.5.0 | N1-030886 |

| Change history |       |           |     |     |  |       |       |           |
|----------------|-------|-----------|-----|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2003-06        | NP-20 | NP-030278 | 387 | 1   | Subscription/Registration refresh time                                     | 5.4.0 | 5.5.0 | N1-030887 |
| 2003-06        | NP-20 | NP-030278 | 388 | 1   | Corrections to use of IK   | 5.4.0 | 5.5.0 | N1-030863 |
| 2003-06        | NP-20 | NP-030278 | 390 |     | Mobile-originating case at UE  | 5.4.0 | 5.5.0 | N1-030647 |
| 2003-06        | NP-20 | NP-030278 | 394 | 2   | Re-authentication procedure.   | 5.4.0 | 5.5.0 | N1-030917 |
| 2003-06        | NP-20 | NP-030278 | 395 |     | Replacement of SIP URL with SIP URI  | 5.4.0 | 5.5.0 | N1-030652 |
| 2003-06        | NP-20 | NP-030279 | 397 | 2   | Notification about registration state                                      | 5.4.0 | 5.5.0 | N1-030926 |
| 2003-06        | NP-20 | NP-030279 | 402 | 1   | Handling of P-Asserted ID in MGCF  | 5.4.0 | 5.5.0 | N1-030848 |
| 2003-06        | NP-20 | NP-030279 | 404 | 1   | S-CSCF initiated release of calls to circuit switched network              | 5.4.0 | 5.5.0 | N1-030873 |
| 2003-06        | NP-20 | NP-030279 | 405 | 2   | Supported Integrity algorithms   | 5.4.0 | 5.5.0 | N1-030927 |
| 2003-06        | NP-20 | NP-030279 | 407 | 1   | RFC 3524, Single Reservation Flows   | 5.4.0 | 5.5.0 | N1-030851 |
| 2003-06        | NP-20 | NP-030279 | 410 | 1   | Clarification of the S-CSCF's handling of the P-access-network-info header | 5.4.0 | 5.5.0 | N1-030868 |
| 2003-06        | NP-20 | NP-030279 | 411 | 2   | Port numbers in the RR header entries                                      | 5.4.0 | 5.5.0 | N1-030941 |
| 2003-06        | NP-20 | NP-030279 | 412 | 2   | Registration abnormal cases  | 5.4.0 | 5.5.0 | N1-030928 |
| 2003-06        | NP-20 | NP-030280 | 415 |     | Minor correction to section 5.4.5.1.2                                      | 5.4.0 | 5.5.0 | N1-030720 |
| 2003-06        | NP-20 | NP-030280 | 417 | 1   | Introduction of RTCP bandwidth   | 5.4.0 | 5.5.0 | N1-030872 |
| 2003-06        | NP-20 | NP-030280 | 418 | 1   | Registratin Event - Shortend   | 5.4.0 | 5.5.0 | N1-030844 |
| 2003-06        | NP-20 | NP-030280 | 419 | 1   | HSS / S-CSCF text relating to user deregistration                          | 5.4.0 | 5.5.0 | N1-030845 |
| 2003-06        | NP-20 | NP-030280 | 421 |     | Handling of unknown methods at the P-CSCF                                  | 5.4.0 | 5.5.0 | N1-030743 |
| 2003-06        | NP-20 | NP-030280 | 422 | 1   | Definitions and abbreviations update                                       | 5.4.0 | 5.5.0 | N1-030870 |
| 2003-06        | NP-20 | NP-030280 | 423 |     | Removal of hanging paragraph   | 5.4.0 | 5.5.0 | N1-030752 |
| 2003-06        | NP-20 | NP-030280 | 424 |     | Access network charging information  | 5.4.0 | 5.5.0 | N1-030753 |
| 2003-06        | NP-20 | NP-030280 | 425 | 1   | UE procedure tidyup  | 5.4.0 | 5.5.0 | N1-030871 |
| 2003-06        | NP-20 | NP-030281 | 426 |     | P-CSCF procedure tidyup  | 5.4.0 | 5.5.0 | N1-030755 |
| 2003-06        | NP-20 | NP-030281 | 427 |     | I-CSCF procedure tidyup  | 5.4.0 | 5.5.0 | N1-030756 |
| 2003-06        | NP-20 | NP-030281 | 428 |     | S-CSCF procedure tidyup  | 5.4.0 | 5.5.0 | N1-030757 |
| 2003-06        | NP-20 | NP-030281 | 429 |     | BGCF procedure tidyup  | 5.4.0 | 5.5.0 | N1-030758 |
| 2003-06        | NP-20 | NP-030281 | 430 |     | AS procedure tidyup  | 5.4.0 | 5.5.0 | N1-030759 |
| 2003-06        | NP-20 | NP-030281 | 431 |     | MRFC procedure tidyup  | 5.4.0 | 5.5.0 | N1-030760 |
| 2003-06        | NP-20 | NP-030281 | 434 | 1   | SDP procedure tidyup   | 5.4.0 | 5.5.0 | N1-030852 |
| 2003-06        | NP-20 | NP-030281 | 438 | 2   | Profile Tables – Further Corrections                                       | 5.4.0 | 5.5.0 | N1-030935 |
| 2003-06        | NP-20 | NP-030281 | 439 | 3   | AS's subscription for the registration state event package                 | 5.4.0 | 5.5.0 | N1-030940 |
| 2003-06        | NP-20 | NP-030281 | 440 |     | Temporary Public User Identity in re- and de-REGISTER requests             | 5.4.0 | 5.5.0 | N1-030792 |
| 2003-09        | NP-21 | NP-030412 | 444 | 2   | All non-REGISTER requests must be integrity protected                      | 5.5.0 | 5.6.0 | N1-031328 |

| Change history |       |           |     |     |  |       |       |           |
|----------------|-------|-----------|-----|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2003-09        | NP-21 | NP-030412 | 445 |     | Download of all service profiles linked to PUID being registered and implicitly registered       | 5.5.0 | 5.6.0 | N1-031010 |
| 2003-09        | NP-21 | NP-030412 | 448 | 3   | Authentication at UE   | 5.5.0 | 5.6.0 | N1-031326 |
| 2003-09        | NP-21 | NP-030412 | 449 | 1   | Network authentication failure at the UE   | 5.5.0 | 5.6.0 | N1-031242 |
| 2003-09        | NP-21 | NP-030412 | 451 | 3   | Handling of security association   | 5.5.0 | 5.6.0 | N1-031327 |
| 2003-09        | NP-21 | NP-030412 | 452 | 1   | Re-authentication timer at S-CSCF  | 5.5.0 | 5.6.0 | N1-031274 |
| 2003-09        | NP-21 | NP-030412 | 455 | 2   | Authentication failure at S-CSCF   | 5.5.0 | 5.6.0 | N1-031285 |
| 2003-09        | NP-21 | NP-030413 | 456 | 2   | Subscription termination sent by the S-CSCF  | 5.5.0 | 5.6.0 | N1-031276 |
| 2003-09        | NP-21 | NP-030413 | 457 |     | Subscription termination at the P-CSCF   | 5.5.0 | 5.6.0 | N1-031032 |
| 2003-09        | NP-21 | NP-030413 | 458 |     | Network -initiated deregistration at P-CSCF  | 5.5.0 | 5.6.0 | N1-031033 |
| 2003-09        | NP-21 | NP-030349 | 459 | 2   | Notification about registration status at AS   | 5.5.0 | 5.6.0 |           |
| 2003-09        | NP-21 | NP-030413 | 461 | 1   | Service profile  | 5.5.0 | 5.6.0 | N1-031233 |
| 2003-09        | NP-21 | NP-030413 | 466 | 1   | Requirements on Preconditions  | 5.5.0 | 5.6.0 | N1-031246 |
| 2003-09        | NP-21 | NP-030413 | 467 | 1   | Call forwarding cleanup  | 5.5.0 | 5.6.0 | N1-031238 |
| 2003-09        | NP-21 | NP-030413 | 468 |     | Update of references   | 5.5.0 | 5.6.0 | N1-031094 |
| 2003-09        | NP-21 | NP-030414 | 470 | 1   | Adding P-Asserted-Identity headers to NE initiated subscriptions                                 | 5.5.0 | 5.6.0 | N1-031314 |
| 2003-09        | NP-21 | NP-030414 | 479 | 1   | Replace USIM by ISIM for user identity storage   | 5.5.0 | 5.6.0 | N1-031247 |
| 2003-09        | NP-21 | NP-030414 | 481 | 1   | 24.229 R5 CR: Corrections to Profile Tables  | 5.5.0 | 5.6.0 | N1-031248 |
| 2003-09        | NP-21 | NP-030414 | 482 |     | 24.229 R5 CR: Setting of SUBSCRIBE expiration time   | 5.5.0 | 5.6.0 | N1-031140 |
| 2003-09        | NP-21 | NP-030414 | 483 | 3   | 24.229 R5 CR: Alignment of IMS Compression with RFC 3486   | 5.5.0 | 5.6.0 | N1-031335 |
| 2003-09        | NP-21 | NP-030418 | 465 | 1   | Alignment with TS for policy control over Gq interface   | 5.6.0 | 6.0.0 | N1-031267 |
| 2003-09        | NP-21 | NP-030418 | 472 | 1   | I-CSCF procedures for openness   | 5.6.0 | 6.0.0 | N1-031304 |
| 2003-09        | NP-21 | NP-030433 | 473 | 3   | Registration from multiple terminals and forking   | 5.6.0 | 6.0.0 |           |
| 2003-09        | NP-21 | NP-030419 | 480 | 3   | Access Independent IMS   | 5.6.0 | 6.0.0 | N1-031333 |
| 2003-12        | NP-22 | NP-030482 | 487 | 1   | Registration amendments in profile   | 6.0.0 | 6.1.0 | N1-031627 |
| 2003-12        | NP-22 | NP-030482 | 489 |     | Privacy considerations for the UE  | 6.0.0 | 6.1.0 | N1-031351 |
| 2003-12        | NP-22 | NP-030476 | 493 |     | INVITE dialog amendments in profile  | 6.0.0 | 6.1.0 | N1-031359 |
| 2003-12        | NP-22 | NP-030482 | 494 |     | Correction of I-CSCF handling of multiple private user identities with same public user identity | 6.0.0 | 6.1.0 | N1-031375 |
| 2003-12        | NP-22 | NP-030476 | 496 | 1   | P-Asserted-Identity in SUBSCRIBE requests  | 6.0.0 | 6.1.0 | N1-031632 |
| 2003-12        | NP-22 | NP-030482 | 497 |     | Addition of reference to Gq interface  | 6.0.0 | 6.1.0 | N1-031378 |
| 2003-12        | NP-22 | NP-030476 | 503 | 2   | Update of HSS information at deregistration  | 6.0.0 | 6.1.0 | N1-031720 |
| 2003-12        | NP-22 | NP-030482 | 507 |     | Unavailable definitions  | 6.0.0 | 6.1.0 | N1-031392 |
| 2003-12        | NP-22 | NP-030476 | 509 |     | Reference corrections  | 6.0.0 | 6.1.0 | N1-031394 |
| 2003-12        | NP-22 | NP-030484 | 510 | 1   | UICC related changes for IMS commonality and interoperability                                    | 6.0.0 | 6.1.0 | N1-031682 |



| Change history |       |           |     |     |   |       |       |           |
|----------------|-------|-----------|-----|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2003-12        | NP-22 | NP-030484 | 511 |     | Interoperability and commonality; definition of scope   | 6.0.0 | 6.1.0 | N1-031427 |
| 2003-12        | NP-22 | NP-030484 | 512 |     | Interoperability and commonality; addition of terminology   | 6.0.0 | 6.1.0 | N1-031428 |
| 2003-12        | NP-22 | NP-030484 | 513 |     | Interoperability and commonality; media grouping  | 6.0.0 | 6.1.0 | N1-031429 |
| 2003-12        | NP-22 | NP-030484 | 515 |     | Interoperability and commonality; charging information  | 6.0.0 | 6.1.0 | N1-031431 |
| 2003-12        | NP-22 | NP-030482 | 518 | 1   | Profile support of RFC 3326: The Reason Header Field for the Session Initiation Protocol                          | 6.0.0 | 6.1.0 | N1-031681 |
| 2003-12        | NP-22 | NP-030482 | 519 |     | Profile support of RFC 3581: An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing | 6.0.0 | 6.1.0 | N1-031439 |
| 2003-12        | NP-22 | NP-030484 | 522 | 1   | Clause 9 restructuring  | 6.0.0 | 6.1.0 | N1-031684 |
| 2003-12        | NP-22 | NP-030477 | 524 | 2   | Correct use of RAND during re-synchronisation failures  | 6.0.0 | 6.1.0 | N1-031712 |
| 2003-12        | NP-22 | NP-030478 | 526 | 1   | Correction to description of RES/XRES usage   | 6.0.0 | 6.1.0 | N1-031617 |
| 2003-12        | NP-22 | NP-030483 | 529 |     | Corrections on charging specification number  | 6.0.0 | 6.1.0 | N1-031469 |
| 2003-12        | NP-22 | NP-030581 | 531 | 3   | Corrections on ICID for REGISTER  | 6.0.0 | 6.1.0 |           |
| 2003-12        | NP-22 | NP-030478 | 543 | 1   | Correction of user initiated re-registration  | 6.0.0 | 6.1.0 | N1-031619 |
| 2003-12        | NP-22 | NP-030483 | 551 | 1   | IMS trust domain in Rel 6   | 6.0.0 | 6.1.0 | N1-031622 |
| 2003-12        | NP-22 | NP-030478 | 556 | 1   | P-CSCF and UE handling of Security Associations   | 6.0.0 | 6.1.0 | N1-031624 |
| 2003-12        | NP-22 | NP-030483 | 560 | 2   | SDP offer handling in SIP responses in S-CSCF and P-CSCF  | 6.0.0 | 6.1.0 | N1-031727 |
| 2003-12        | NP-22 | NP-030483 | 564 | 1   | SIP compression   | 6.0.0 | 6.1.0 | N1-031705 |
| 2003-12        | NP-22 | NP-030478 | 566 |     | Sending challenge   | 6.0.0 | 6.1.0 | N1-031580 |
| 2003-12        | NP-22 | NP-030480 | 568 | 2   | Reg-await-auth timer value  | 6.0.0 | 6.1.0 | N1-031716 |
| 2003-12        | NP-22 | NP-030480 | 571 | 1   | Network initiated deregistration  | 6.0.0 | 6.1.0 | N1-031707 |
| 2003-12        | NP-22 | NP-030483 | 572 |     | Text harmonisation with 3GPP2   | 6.0.0 | 6.1.0 | N1-031589 |
| 2003-12        | NP-22 | NP-030483 | 573 | 1   | Procedures in the absence of UICC   | 6.0.0 | 6.1.0 | N1-031680 |
| 2003-12        | NP-22 | NP-030483 | 575 | 1   | P-Access-Network-Info changes   | 6.0.0 | 6.1.0 | N1-031683 |
| 2004-03        | NP-23 | NP-040027 | 488 | 3   | Completion of major capabilities table in respect of privacy  | 6.1.0 | 6.2.0 | N1-040406 |
| 2004-03        | NP-23 | NP-040027 | 499 | 5   | P-CSCF integrity protection   | 6.1.0 | 6.2.0 | N1-040500 |
| 2004-03        | NP-23 | NP-040032 | 578 | 1   | UE requesting no-fork   | 6.1.0 | 6.2.0 | N1-040184 |
| 2004-03        | NP-23 | NP-040032 | 579 | 1   | Inclusion of caller preferences into profile  | 6.1.0 | 6.2.0 | N1-040284 |
| 2004-03        | NP-23 | NP-040027 | 586 | 1   | Network-initiated re-authentication   | 6.1.0 | 6.2.0 | N1-040391 |
| 2004-03        | NP-23 | NP-040032 | 588 | 1   | Re-authentication - Abnormal cases  | 6.1.0 | 6.2.0 | N1-040393 |
| 2004-03        | NP-23 | NP-040027 | 592 | 1   | Integrity protected correction  | 6.1.0 | 6.2.0 | N1-040398 |
| 2004-03        | NP-23 | NP-040032 | 596 | 1   | Sec-agree parameter in "Proxy-Require" header   | 6.1.0 | 6.2.0 | N1-040400 |
| 2004-03        | NP-23 | NP-040027 | 600 | 2   | Handling of record-route in target refresh and subsequent request   | 6.1.0 | 6.2.0 | N1-040481 |
| 2004-03        | NP-23 | NP-040035 | 603 |     | Cleanup for IP-CAN and GPRS   | 6.1.0 | 6.2.0 | N1-040304 |

| Change history |       |           |     |     |  |       |       |           |
|----------------|-------|-----------|-----|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2004-03        | NP-23 | NP-040032 | 604 |     | Forking in S-CSCF  | 6.1.0 | 6.2.0 | N1-040325 |
| 2004-03        | NP-23 | NP-040108 | 605 | 3   | Determination of S-CSCF role   | 6.1.0 | 6.2.0 |           |
| 2004-03        | NP-23 | NP-040134 | 608 | 3   | Unprotected deregistration   | 6.1.0 | 6.2.0 |           |
| 2004-03        | NP-23 | NP-040029 | 610 |     | Sending authentication challenge   | 6.1.0 | 6.2.0 | N1-040331 |
| 2004-03        | NP-23 | NP-040033 | 613 |     | Reference to PDF operation   | 6.1.0 | 6.2.0 | N1-040334 |
| 2004-03        | NP-23 | NP-040029 | 615 | 1   | Support of MESSAGE (Profile Tables)                                      | 6.1.0 | 6.2.0 | N1-040466 |
| 2004-03        | NP-23 | NP-040033 | 616 | 2   | Introduction of PSI Routing to 24.229                                    | 6.1.0 | 6.2.0 | N1-040487 |
| 2004-03        | NP-23 | NP-040033 | 617 | 1   | P-CSCF Re-selection  | 6.1.0 | 6.2.0 | N1-040463 |
| 2004-03        | NP-23 | NP-040033 | 618 |     | I-CSCF does not re-select S-CSCF during re-registration                  | 6.1.0 | 6.2.0 | N1-040344 |
| 2004-03        | NP-23 | NP-040033 | 620 | 1   | Handling of media authorization token due to messaging                   | 6.1.0 | 6.2.0 | N1-040430 |
| 2004-06        | NP-24 | NP-040191 | 621 | 2   | Forking requests terminating at the served user                          | 6.2.0 | 6.3.0 | N1-040739 |
| 2004-06        | NP-24 | NP-040191 | 624 | 1   | Abbreviations  | 6.2.0 | 6.3.0 | N1-040691 |
| 2004-06        | NP-24 | NP-040191 | 625 | 5   | Removal of restriction for multiple SIP sessions on a single PDP context | 6.2.0 | 6.3.0 | N1-041053 |
| 2004-06        | NP-24 | NP-040191 | 626 | 3   | Record route in S-CSCF   | 6.2.0 | 6.3.0 | N1-041061 |
| 2004-06        | NP-24 | NP-040189 | 627 | 3   | Correction of reception of media authorization token                     | 6.2.0 | 6.3.0 | N1-040994 |
| 2004-06        | NP-24 | NP-040191 | 628 | 3   | Introduction of PSI Routing to 24.229                                    | 6.2.0 | 6.3.0 | N1-041059 |
| 2004-06        | NP-24 | NP-040198 | 629 | 2   | Addition of PRESNC material  | 6.2.0 | 6.3.0 | N1-040996 |
| 2004-06        | NP-24 | NP-040189 | 631 | 1   | Missing statements regarding P-Charging-Function-Addresses header        | 6.2.0 | 6.3.0 | N1-040987 |
| 2004-06        | NP-24 | NP-040191 | 634 | 1   | Multiple registrations   | 6.2.0 | 6.3.0 | N1-041054 |
| 2004-06        | NP-24 | NP-040192 | 635 | 1   | Network-initiated deregistration   | 6.2.0 | 6.3.0 | N1-041055 |
| 2004-06        | NP-24 | NP-040192 | 636 |     | Network-initiated re-authentication                                      | 6.2.0 | 6.3.0 | N1-040778 |
| 2004-06        | NP-24 | NP-040192 | 637 | 1   | Mobile-initiated deregistration  | 6.2.0 | 6.3.0 | N1-041056 |
| 2004-06        | NP-24 | NP-040192 | 638 | 1   | Notification about registration state                                    | 6.2.0 | 6.3.0 | N1-041057 |
| 2004-06        | NP-24 | NP-040189 | 642 | 3   | Syntax of the extension to the P-Charging-Vector header field            | 6.2.0 | 6.3.0 | N1-041100 |
| 2004-06        | NP-24 | NP-040192 | 643 | 2   | Session Timer  | 6.2.0 | 6.3.0 | N1-041095 |
| 2004-06        | NP-24 | NP-040193 | 644 | 3   | Session initiation without preconditions                                 | 6.2.0 | 6.3.0 | N1-041096 |
| 2004-06        | NP-24 | NP-040192 | 645 | 1   | IMS Conferencing: Inclusion of Profile Tables to TS 24.229               | 6.2.0 | 6.3.0 | N1-041015 |
| 2004-06        | NP-24 | NP-040189 | 649 | 1   | Revisions due to published version of draft-ietf-sipping-reg-event       | 6.2.0 | 6.3.0 | N1-040992 |
| 2004-06        | NP-24 | NP-040198 | 652 |     | Creation of separate event package table for UA role                     | 6.2.0 | 6.3.0 | N1-041066 |
| 2004-09        | NP-25 | NP-040380 | 658 |     | Correction of User identity verification at the AS                       | 6.3.0 | 6.4.0 | N1-041344 |
| 2004-09        | NP-25 | NP-040381 | 666 | 1   | NOTIFY requests  | 6.3.0 | 6.4.0 | N1-041586 |
| 2004-09        | NP-25 | NP-040381 | 654 | 4   | Callee capabilities and Registration                                     | 6.3.0 | 6.4.0 | N1-041315 |

| Change history |       |           |     |     |   |       |       |           |
|----------------|-------|-----------|-----|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2004-09        | NP-25 | NP-040381 | 668 | 2   | Network deregistration  | 6.3.0 | 6.4.0 | N1-041614 |
| 2004-09        | NP-25 | NP-040381 | 682 | 1   | SDP parameters received by the S-CSCF and the P-CSCF in the 200 OK message                              | 6.3.0 | 6.4.0 | N1-041592 |
| 2004-09        | NP-25 | NP-040381 | 661 | 1   | Call Release  | 6.3.0 | 6.4.0 | N1-041589 |
| 2004-09        | NP-25 | NP-040381 | 659 |     | Multiple public ID registration   | 6.3.0 | 6.4.0 | N1-041350 |
| 2004-09        | NP-25 | NP-040381 | 660 |     | Standalone transactions   | 6.3.0 | 6.4.0 | N1-041351 |
| 2004-09        | NP-25 | NP-040381 | 663 |     | Unprotected REGISTER  | 6.3.0 | 6.4.0 | N1-041354 |
| 2004-09        | NP-25 | NP-040381 | 662 | 1   | Session timer   | 6.3.0 | 6.4.0 | N1-041590 |
| 2004-09        | NP-25 | NP-040381 | 665 |     | Contact in SUBSCRIBE request  | 6.3.0 | 6.4.0 | N1-041372 |
| 2004-09        | NP-25 | NP-040381 | 650 | 2   | Support of draft-ietf-sip-replaces  | 6.3.0 | 6.4.0 | N1-041391 |
| 2004-09        | NP-25 | NP-040381 | 657 | 1   | Support of draft-ietf-sip-join  | 6.3.0 | 6.4.0 | N1-041393 |
| 2004-09        | NP-25 | NP-040381 | 656 | 1   | Support of draft-ietf-sip-referredby  | 6.3.0 | 6.4.0 | N1-041263 |
| 2004-09        | NP-25 | NP-040381 | 678 |     | Support of TLS  | 6.3.0 | 6.4.0 | N1-041462 |
| 2004-09        | NP-25 | NP-040381 | 688 | 2   | Filtering of the P-Access-Network-Info header by the S-CSCF and privacy rules                           | 6.3.0 | 6.4.0 | N1-041641 |
| 2004-09        | NP-25 | NP-040382 | 692 | 2   | Ipv6 Ipv4 interworking  | 6.3.0 | 6.4.0 | N1-041630 |
| 2004-09        | NP-25 | NP-040383 | 689 | 2   | Addition of session set-up not requiring preconditions and reliable transport of provisional responses. | 6.3.0 | 6.4.0 | N1-041632 |
| 2004-09        | NP-25 | NP-040385 | 697 |     | Missing value for the event attribute within the <contact> element of NOTIFY body                       | 6.3.0 | 6.4.0 | N1-041540 |
| 2004-09        | NP-25 | NP-040385 | 698 |     | HSS initiated deregistration  | 6.3.0 | 6.4.0 | N1-041549 |
| 2004-09        | NP-25 | NP-040385 | 673 |     | Syntax correction for the P-Charging-Vector header  | 6.3.0 | 6.4.0 | N1-041434 |
| 2004-09        | NP-25 | NP-040385 | 699 | 1   | Network initiated deregistration upon UE roaming and registration to a new network                      | 6.3.0 | 6.4.0 | N1-041629 |
| 2004-12        | NP-26 | NP-040506 | 651 | 4   | Downloading the user profile based on User-Data-Request-Type  | 6.4.0 | 6.5.0 | N1-042031 |
| 2004-12        | NP-26 | NP-040506 | 703 | 2   | SDP Encryption  | 6.4.0 | 6.5.0 | N1-042095 |
| 2004-12        | NP-26 | NP-040506 | 704 | 1   | RTCP streams  | 6.4.0 | 6.5.0 | N1-042019 |
| 2004-12        | NP-26 | NP-040506 | 709 |     | Contact in 200(OK) response   | 6.4.0 | 6.5.0 | N1-041725 |
| 2004-12        | NP-26 | NP-040506 | 710 | 1   | P-Access-Network-Info header  | 6.4.0 | 6.5.0 | N1-042020 |
| 2004-12        | NP-26 | NP-040506 | 711 | 1   | P-Called-Party-ID header  | 6.4.0 | 6.5.0 | N1-041954 |
| 2004-12        | NP-26 | NP-040506 | 713 | 1   | IMS-ALG routing   | 6.4.0 | 6.5.0 | N1-042021 |
| 2004-12        | NP-26 | NP-040506 | 714 | 1   | Public User Identity  | 6.4.0 | 6.5.0 | N1-042022 |
| 2004-12        | NP-26 | NP-040506 | 715 | 1   | "Pres" and "im" URIs  | 6.4.0 | 6.5.0 | N1-042023 |
| 2004-12        | NP-26 | NP-040502 | 723 | 1   | Correction Term IOI handling  | 6.4.0 | 6.5.0 | N1-041956 |
| 2004-12        | NP-26 | NP-040502 | 725 | 1   | Request handling in S-CSCF originating case   | 6.4.0 | 6.5.0 | N1-041958 |
| 2004-12        | NP-26 | NP-040502 | 727 | 1   | Request handling in S-CSCF - terminating case   | 6.4.0 | 6.5.0 | N1-041960 |
| 2004-12        | NP-26 | NP-040506 | 728 |     | SBLP and non-realtime PDP contexts  | 6.4.0 | 6.5.0 | N1-041797 |
| 2004-12        | NP-26 | NP-040590 | 730 | 2   | Reference updates   | 6.4.0 | 6.5.0 | N1-042085 |

| Change history |       |           |     |     |   |        |        |           |
|----------------|-------|-----------|-----|-----|---|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment   | Old    | New    | WG doc    |
| 2004-12        | NP-26 | NP-040590 | 733 | 3   | Support for extended SigComp  | 6.4.0  | 6.5.0  | N1-042117 |
| 2004-12        | NP-26 | NP-040590 | 734 | 2   | Correction to subclause 5.1.3 of TS 24,229  | 6.4.0  | 6.5.0  | N1-042120 |
| 2004-12        | NP-26 | NP-040590 | 735 | 1   | Correction to subclause 5.1.4.1.2.3 of TS 24,229  | 6.4.0  | 6.5.0  | N1-042084 |
| 2004-12        | NP-26 | NP-040502 | 738 | 1   | Population of Via header when using REGISTER method   | 6.4.0  | 6.5.0  | N1-041962 |
| 2004-12        | NP-26 | NP-040590 | 739 |     | Tel-URI related reference updates   | 6.4.0  | 6.5.0  | N1-041869 |
| 2004-12        | NP-26 | NP-040590 | 741 | 1   | Throttling  | 6.4.0  | 6.5.0  | N1-042086 |
| 2004-12        | NP-26 | NP-040590 | 742 |     | Editorial correction resulting from CR665   | 6.4.0  | 6.5.0  | N1-041881 |
| 2004-12        | NP-26 | NP-040590 | 743 |     | Unprotected REGISTER corrections  | 6.4.0  | 6.5.0  | N1-041882 |
| 2004-12        | NP-26 | NP-040590 | 744 | 1   | Corrections to receiving SDP offer in 200 (OK) response   | 6.4.0  | 6.5.0  | N1-042087 |
| 2004-12        | NP-26 | NP-040590 | 745 | 1   | Privacy corrections   | 6.4.0  | 6.5.0  | N1-042085 |
| 2004-12        | NP-26 | NP-040590 | 747 | 2   | Syntax of the P-Charging-Vector   | 6.4.0  | 6.5.0  | N1-042105 |
| 2004-12        | NP-26 | NP-040590 | 752 | 2   | Unavailability of the access-network-charging-info when the session is established without SBLP   | 6.4.0  | 6.5.0  | N1-042106 |
| 2004-12        | NP-26 | NP-040590 | 753 | 1   | SIP messages carrying the access-network-charging-info for sessions without preconditions   | 6.4.0  | 6.5.0  | N1-042089 |
| 2004-12        | NP-26 | NP-040590 | 755 | 1   | Network-initiated deregistration for multiple UEs sharing the same user public identity and for the old contact information of a roaming UE registered in a new network | 6.4.0  | 6.5.0  | N1-042090 |
| 2004-12        | NP-26 | NP-040502 | 765 | 1   | Interaction between S-CSCF and HSS in Network initiated deregistration procedure  | 6.4.0  | 6.5.0  | N1-041966 |
| 2004-12        | NP-26 | NP-040502 | 768 | 1   | Downloading of user profile   | 6.4.0  | 6.5.0  | N1-042103 |
| 2005-01        |       |           |     |     | Fix Word problem  | 6.5.0  | 6.5.1  |           |
| 2005-03        | NP-27 | NP-050069 | 839 |     | Filter criteria matching and generation of third-party REGISTER request for network-initiated deregistration  | 5.11.1 | 5.12.0 | N1-050220 |
| 2005-03        | NP-27 | NP-050069 | 785 |     | Deregistration effect on active sessions  | 6.5.1  | 6.6.0  | N1-050052 |
| 2005-03        | NP-27 | NP-050069 | 784 |     | Deregistration effect on active sessions  | 5.11.1 | 5.12.0 | N1-050051 |
| 2005-03        | NP-27 | NP-050069 | 809 | 1   | IOI storage at MGCF   | 5.11.1 | 5.12.0 | N1-050295 |
| 2005-03        | NP-27 | NP-050069 | 840 |     | Filter criteria matching and generation of third-party REGISTER request for network-initiated deregistration  | 6.5.1  | 6.6.0  | N1-050221 |
| 2005-03        | NP-27 | NP-050069 | 806 | 1   | Use of original dialog identifier at AS   | 6.5.1  | 6.6.0  | N1-050292 |
| 2005-03        | NP-27 | NP-050069 | 807 | 2   | Checking Request-URI for terminating requests at the S-CSCF   | 5.11.1 | 5.12.0 | N1-050401 |
| 2005-03        | NP-27 | NP-050069 | 805 | 1   | Use of original dialog identifier at AS   | 5.11.1 | 5.12.0 | N1-050291 |
| 2005-03        | NP-27 | NP-050069 | 808 | 2   | Checking Request-URI for terminating requests at the S-CSCF   | 6.5.1  | 6.6.0  | N1-050402 |
| 2005-03        | NP-27 | NP-050069 | 810 | 1   | IOI storage at MGCF   | 6.5.1  | 6.6.0  | N1-050296 |
| 2005-03        | NP-27 | NP-050073 | 794 |     | RFC 3966  | 6.5.1  | 6.6.0  | N1-050080 |
| 2005-03        | NP-27 | NP-050073 | 848 | 1   | Removal of I-CSCF normative requirement on Cx interface   | 6.5.1  | 6.6.0  | N1-050299 |

| Change history |       |           |     |     |   |       |       |           |
|----------------|-------|-----------|-----|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2005-03        | NP-27 | NP-050073 | 841 |     | Filtering of the P-Access-Network-Info header by the S-CSCF and privacy rules   | 6.5.1 | 6.6.0 | N1-050225 |
| 2005-03        | NP-27 | NP-050073 | 817 |     | Editorial corrections   | 6.5.1 | 6.6.0 | N1-050129 |
| 2005-03        | NP-27 | NP-050073 | 786 | 1   | Cleanups resulting from CR changes for last version   | 6.5.1 | 6.6.0 | N1-050324 |
| 2005-03        | NP-27 | NP-050073 | 821 | 1   | Handling topmost Route header at the P-CSCF   | 6.5.1 | 6.6.0 | N1-050297 |
| 2005-03        | NP-27 | NP-050073 | 790 |     | Registration - Abnormal Case  | 6.5.1 | 6.6.0 | N1-050076 |
| 2005-03        | NP-27 | NP-050074 | 832 | 1   | Corrections to the tables for 'PUBLISH'   | 6.5.1 | 6.6.0 | N1-050341 |
| 2005-03        | NP-27 | NP-050074 | 822 | 1   | Corrections to the UE tables for 'major capabilities'   | 6.5.1 | 6.6.0 | N1-050332 |
| 2005-03        | NP-27 | NP-050074 | 825 | 1   | Corrections to the UE tables for 'ACK'  | 6.5.1 | 6.6.0 | N1-050334 |
| 2005-03        | NP-27 | NP-050074 | 826 | 1   | Corrections to the tables for 'CANCEL'  | 6.5.1 | 6.6.0 | N1-050335 |
| 2005-03        | NP-27 | NP-050074 | 827 | 1   | Corrections to the tables for 'INVITE'  | 6.5.1 | 6.6.0 | N1-050336 |
| 2005-03        | NP-27 | NP-050074 | 828 | 1   | Corrections to the tables for 'MESSAGE'   | 6.5.1 | 6.6.0 | N1-050337 |
| 2005-03        | NP-27 | NP-050074 | 829 | 1   | Corrections to the tables for 'NOTIFY'  | 6.5.1 | 6.6.0 | N1-050338 |
| 2005-03        | NP-27 | NP-050074 | 830 | 1   | Corrections to the tables for 'OPTIONS'   | 6.5.1 | 6.6.0 | N1-050339 |
| 2005-03        | NP-27 | NP-050074 | 834 | 1   | Corrections to the tables for 'REGISTER'  | 6.5.1 | 6.6.0 | N1-050343 |
| 2005-03        | NP-27 | NP-050074 | 831 | 1   | Corrections to the tables for 'PRACK'   | 6.5.1 | 6.6.0 | N1-050340 |
| 2005-03        | NP-27 | NP-050074 | 833 | 1   | Corrections to the tables for 'REFER'   | 6.5.1 | 6.6.0 | N1-050342 |
| 2005-03        | NP-27 | NP-050074 | 835 | 1   | Corrections to the tables for 'SUBSCRIBE'   | 6.5.1 | 6.6.0 | N1-050344 |
| 2005-03        | NP-27 | NP-050074 | 836 | 1   | Corrections to the tables for 'UPDATE'  | 6.5.1 | 6.6.0 | N1-050345 |
| 2005-03        | NP-27 | NP-050074 | 837 | 1   | Corrections to the tables for SDP   | 6.5.1 | 6.6.0 | N1-050346 |
| 2005-03        | NP-27 | NP-050074 | 824 | 1   | Removal of the UE table for 'status codes'  | 6.5.1 | 6.6.0 | N1-050351 |
| 2005-03        | NP-27 | NP-050074 | 823 | 1   | Corrections to the tables for 'BYE'   | 6.5.1 | 6.6.0 | N1-050333 |
| 2005-03        | NP-27 | NP-050075 | 846 | 2   | Correction to the Registration procedure  | 6.5.1 | 6.6.0 | N1-050413 |
| 2005-03        | NP-27 | NP-050075 | 850 | 1   | Addition of IMS-ALF to profile tables   | 6.5.1 | 6.6.0 | N1-050348 |
| 2005-03        | NP-27 | NP-050075 | 851 | 2   | Press and im URIs in incoming requests  | 6.5.1 | 6.6.0 | N1-050395 |
| 2005-03        | NP-27 | NP-050075 | 788 | 1   | MO - Calls to IPv4 SIP terminals  | 6.5.1 | 6.6.0 | N1-050387 |
| 2005-03        | NP-27 | NP-050075 | 818 | 3   | Corrections to subclause 5.5 in TS 24.229   | 6.5.1 | 6.6.0 | N1-050414 |
| 2005-03        | NP-27 | NP-050075 | 801 | 3   | Default handling associated with the trigger at the S-CSCF  | 6.5.1 | 6.6.0 | N1-050418 |
| 2005-03        | NP-27 | NP-050075 | 803 | 4   | Default handling associated with the trigger for third party registration   | 6.5.1 | 6.6.0 | N1-050421 |
| 2005-03        | NP-27 | NP-050078 | 795 | 1   | Sip-profile package in major capabilities   | 6.5.1 | 6.6.0 | N1-050306 |
| 2005-03        | NP-27 | NP-050127 | 849 | 2   | Corrections to addition of session set-up not requiring preconditions and reliable transport of provisional responses | 6.5.1 | 6.6.0 |           |
| 2005-06        | CP-28 | CP-050059 | 879 |     | Correction Reg-Await-Auth Timer   | 6.6.0 | 6.7.0 | C1-050522 |
| 2005-06        | CP-28 | CP-050059 | 881 |     | Security Association in P-CSCF  | 6.6.0 | 6.7.0 | C1-050524 |
| 2005-06        | CP-28 | CP-050059 | 871 | 1   | Port 5060   | 6.6.0 | 6.7.0 | C1-050674 |

| Change history |       |           |     |     |   |       |       |           |
|----------------|-------|-----------|-----|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR  | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2005-06        | CP-28 | CP-050059 | 891 | 2   | SIP headers storage for P-CSCF initiated session release  | 6.6.0 | 6.7.0 | C1-050777 |
| 2005-06        | CP-28 | CP-050059 | 921 | 1   | Correction of error in the specification of the extension to Authorization header                 | 6.6.0 | 6.7.0 | C1-050689 |
| 2005-06        | CP-28 | CP-050059 | 886 | 2   | Handling of P-Associated URI header   | 6.6.0 | 6.7.0 | C1-050783 |
| 2005-06        | CP-28 | CP-050059 | 907 | 2   | Clarification to the procedures at the I-CSCF   | 6.6.0 | 6.7.0 | C1-050785 |
| 2005-06        | CP-28 | CP-050061 | 894 | 1   | Re-registration failure   | 6.6.0 | 6.7.0 | C1-050709 |
| 2005-06        | CP-28 | CP-050061 | 892 |     | Completion of status-code tables in SIP profile   | 6.6.0 | 6.7.0 | C1-050571 |
| 2005-06        | CP-28 | CP-050061 | 865 | 1   | Unsubscribe by P-CSCF   | 6.6.0 | 6.7.0 | C1-050671 |
| 2005-06        | CP-28 | CP-050061 | 866 | 1   | Protected initial registration  | 6.6.0 | 6.7.0 | C1-050708 |
| 2005-06        | CP-28 | CP-050061 | 916 | 1   | Clarify that S-CSCF shall support Supported and Require headers                                   | 6.6.0 | 6.7.0 | C1-050684 |
| 2005-06        | CP-28 | CP-050061 | 862 |     | Shared public user identities   | 6.6.0 | 6.7.0 | C1-050599 |
| 2005-06        | CP-28 | CP-050061 | 860 | 1   | P-CSCF - routing of REGISTER requests   | 6.6.0 | 6.7.0 | C1-050701 |
| 2005-06        | CP-28 | CP-050061 | 870 | 1   | Correction of table A.104A  | 6.6.0 | 6.7.0 | C1-050711 |
| 2005-06        | CP-28 | CP-050061 | 887 | 1   | Contact address in REGISTER response  | 6.6.0 | 6.7.0 | C1-050716 |
| 2005-06        | CP-28 | CP-050061 | 890 | 1   | P-CSCF Record-Route processing for target refresh requests/responses                              | 6.6.0 | 6.7.0 | C1-050717 |
| 2005-06        | CP-28 | CP-050061 | 893 | 1   | AS originated requests on behalf of PSI   | 6.6.0 | 6.7.0 | C1-050719 |
| 2005-06        | CP-28 | CP-050061 | 896 | 1   | Routing PSI at terminating side   | 6.6.0 | 6.7.0 | C1-050720 |
| 2005-06        | CP-28 | CP-050061 | 856 | 2   | Notification about registration state   | 6.6.0 | 6.7.0 | C1-050789 |
| 2005-06        | CP-28 | CP-050061 | 861 | 3   | Registration failure at UE  | 6.6.0 | 6.7.0 | C1-050790 |
| 2005-06        | CP-28 | CP-050061 | 899 | 2   | Correction of the references for the integration of resource management procedures                | 6.6.0 | 6.7.0 | C1-050791 |
| 2005-06        | CP-28 | CP-050061 | 902 | 2   | Clarification on P-CSCF-initiated call release  | 6.6.0 | 6.7.0 | C1-050792 |
| 2005-06        | CP-28 | CP-050061 | 863 | 3   | Error handling in UE in case of RFC 3524  | 6.6.0 | 6.7.0 | C1-050793 |
| 2005-06        | CP-28 | CP-050061 | 895 | 3   | UE registration failure because the selected S-CSCF is unreachable                                | 6.6.0 | 6.7.0 | C1-050802 |
| 2005-06        | CP-28 | CP-050061 | 787 | 6   | MT- SDP offer with IPv4 address.  | 6.6.0 | 6.7.0 | C1-050794 |
| 2005-06        | CP-28 | CP-050061 | 858 | 1   | S-CSCF redirecting  | 6.6.0 | 6.7.0 | C1-050700 |
| 2005-06        | CP-28 | CP-050064 | 872 | 2   | I-WLAN information for IMS  | 6.6.0 | 6.7.0 | C1-050729 |
| 2005-06        | CP-28 | CP-050074 | 901 |     | MWI RFC3842   | 6.6.0 | 7.0.0 | C1-050600 |
| 2005-06        | CP-28 | CP-050075 | 905 | 1   | 3xx response and non-SDP bodies handling by proxies   | 6.6.0 | 7.0.0 | C1-050775 |
| 2005-09        | CP-29 | CP-050346 | 986 |     | Modifications to 24.229 to allow multiple IPsec security association per IKE_Security association | 7.0.0 | 7.1.0 |           |
| 2005-09        | CP-29 | CP-050355 | 930 | 1   | Correction Profile Table A.119  | 7.0.0 | 7.1.0 | C1-051061 |
| 2005-09        | CP-29 | CP-050355 | 946 |     | Public User identity in 3rd party REG   | 7.0.0 | 7.1.0 | C1-050906 |
| 2005-09        | CP-29 | CP-050355 | 957 | 1   | Removal of Access Network Charging Information by the S-CSCF                                      | 7.0.0 | 7.1.0 | C1-051081 |
| 2005-09        | CP-29 | CP-050355 | 965 |     | Optional ccf  | 7.0.0 | 7.1.0 | C1-050986 |

| Change history |       |           |      |     |   |       |       |           |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2005-09        | CP-29 | CP-050355 | 969  | 1   | Contact header in REGISTER requests   | 7.0.0 | 7.1.0 | C1-051177 |
| 2005-09        | CP-29 | CP-050359 | 932  |     | SigComp-Corrections   | 7.0.0 | 7.1.0 | C1-050877 |
| 2005-09        | CP-29 | CP-050359 | 962  | 1   | IETF reference corrections  | 7.0.0 | 7.1.0 | C1-051074 |
| 2005-09        | CP-29 | CP-050359 | 968  | 1   | AS procedure correction   | 7.0.0 | 7.1.0 | C1-051085 |
| 2005-09        | CP-29 | CP-050367 | 924  |     | Incorporation of draft-ietf-sip-history   | 7.0.0 | 7.1.0 | C1-050838 |
| 2005-09        | CP-29 | CP-050367 | 938  |     | Contact header  | 7.0.0 | 7.1.0 | C1-050887 |
| 2005-09        | CP-29 | CP-050367 | 939  | 1   | Reason header - loss of radio coverage  | 7.0.0 | 7.1.0 | C1-051158 |
| 2005-09        | CP-29 | CP-050367 | 947  | 3   | Changes to TS 24.229 to ease interworking with non precondition terminals               | 7.0.0 | 7.1.0 | C1-051213 |
| 2005-09        | CP-29 | CP-050367 | 958  | 2   | Contents of P-Associated-URI header in 200 (OK) response to REGISTER                    | 7.0.0 | 7.1.0 | C1-051206 |
| 2005-09        | CP-29 | CP-050367 | 960  | 3   | Consideration on 3rd Party Service Provider in Trust Domain                             | 7.0.0 | 7.1.0 | C1-051208 |
| 2005-09        | CP-29 | CP-050367 | 971  | 1   | Correction of requirement to insert P-Asserted-Identity header                          | 7.0.0 | 7.1.0 | C1-051166 |
| 2005-09        | CP-29 | CP-050368 | 950  | 3   | privacy and trust rules for History header  | 7.0.0 | 7.1.0 | C1-051199 |
| 2005-10        |       |           |      |     | missing word in subclause 5.4.1.2.2, bullet 10b) is added by MCC                        | 7.1.0 | 7.1.1 |           |
| 2005-12        | CP-30 | CP-050538 | 1049 |     | Replace "originated" with "terminated"  | 7.1.1 | 7.2.0 | C1-051479 |
| 2005-12        | CP-30 | CP-050538 | 1046 | 2   | Mobile originating call related requests  | 7.1.1 | 7.2.0 | C1-051668 |
| 2005-12        | CP-30 | CP-050538 | 1012 | 1   | Correction to section 5.4.3.2 t of TS 24.229  | 7.1.1 | 7.2.0 | C1-051563 |
| 2005-12        | CP-30 | CP-050538 | 1026 |     | Handling of P-Charging-Function-Address   | 7.1.1 | 7.2.0 | C1-051424 |
| 2005-12        | CP-30 | CP-050538 | 1071 |     | Correction Syntax P-Charging Vector   | 7.1.1 | 7.2.0 | C1-051508 |
| 2005-12        | CP-30 | CP-050541 | 1002 | 1   | Modification to the definition of Security Association                                  | 7.1.1 | 7.2.0 | C1-051576 |
| 2005-12        | CP-30 | CP-050542 | 0982 | 3   | Access Type of P-Access-Network-Info header   | 7.1.1 | 7.2.0 | C1-051675 |
| 2005-12        | CP-30 | CP-050542 | 1059 |     | Replace "served" by "Originating" UE  | 7.1.1 | 7.2.0 | C1-051489 |
| 2005-12        | CP-30 | CP-050542 | 1017 |     | Correction to subclause 5.7.5.1. of TS 24229  | 7.1.1 | 7.2.0 | C1-051382 |
| 2005-12        | CP-30 | CP-050542 | 1073 | 2   | Short Session Setup in IMS  | 7.1.1 | 7.2.0 | C1-051656 |
| 2005-12        | CP-30 | CP-050542 | 1054 |     | Adjusting section reference in section 6.3  | 7.1.1 | 7.2.0 | C1-051484 |
| 2005-12        | CP-30 | CP-050542 | 1029 | 1   | B2B UA AS handling  | 7.1.1 | 7.2.0 | C1-041597 |
| 2005-12        | CP-30 | CP-050542 | 1062 | 2   | Correction to 3rd party registration procedures for SESSION_TERMINATED default handling | 7.1.1 | 7.2.0 | C1-051672 |
| 2005-12        | CP-30 | CP-050542 | 0994 |     | cdma2000  | 7.1.1 | 7.2.0 | C1-051336 |
| 2005-12        | CP-30 | CP-050542 | 1043 |     | Correction of a reference in some tables in Appendix A                                  | 7.1.1 | 7.2.0 | C1-051473 |
| 2005-12        | CP-30 | CP-050542 | 1005 | 2   | Refreshes of SUBSCRIBE to reg-event (Fix for Rel 7)                                     | 7.1.1 | 7.2.0 | C1-051670 |
| 2005-12        | CP-30 | CP-050542 | 1065 | 1   | Charging terms correction   | 7.1.1 | 7.2.0 | C1-051618 |
| 2005-12        | CP-30 | CP-050548 | 1081 |     | Change of originating and terminating terminal terminology                              | 7.1.1 | 7.2.0 | C1-051535 |
| 2005-12        | CP-30 | CP-050548 | 1069 | 2   | IBCF  | 7.1.1 | 7.2.0 | C1-051587 |

| Change history |       |           |      |     |   |       |       |           |  |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|--|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |  |
| 2005-12        | CP-30 | CP-050550 | 1055 |     | Editorial Changes   | 7.1.1 | 7.2.0 | C1-051485 |  |
| 2005-12        | CP-30 | CP-050550 | 0996 | 1   | UE initiated deregistration   | 7.1.1 | 7.2.0 | C1-051649 |  |
| 2005-12        | CP-30 | CP-050550 | 1027 | 1   | Mobile originated Request for unregistered user                                       | 7.1.1 | 7.2.0 | C1-051653 |  |
| 2005-12        | CP-30 | CP-050550 | 0990 | 1   | Authentication related Clarification  | 7.1.1 | 7.2.0 | C1-051560 |  |
| 2005-12        | CP-30 | CP-050550 | 1019 | 2   | Receipt of SIP URI with user equal phone at I-CSCF                                    | 7.1.1 | 7.2.0 | C1-051671 |  |
| 2005-12        | CP-30 | CP-050550 | 0995 | 2   | Default public user ID  | 7.1.1 | 7.2.0 | C1-051691 |  |
| 2005-12        | CP-30 | CP-050550 | 0997 | 1   | P-Preferred-Identity header   | 7.1.1 | 7.2.0 | C1-051650 |  |
| 2005-12        | CP-30 | CP-050550 | 1082 | 1   | P-CSCF discovery  | 7.1.1 | 7.2.0 | C1-051681 |  |
| 2005-12        | CP-30 | CP-050677 | 1085 | 2   | Incorporating of TR 24.819 fixed broadband access impacts into TS 24.229              | 7.1.1 | 7.2.0 |           |  |
| 2006-03        | CP-31 | CP-060106 | 1187 | -   | Removal of Warning header non-compliance with RFC 3261                                | 7.2.0 | 7.3.0 | C1-060328 |  |
| 2006-03        | CP-31 | CP-060106 | 1117 | 1   | IMS AKA - SQN resync clarifications   | 7.2.0 | 7.3.0 | C1-060453 |  |
| 2006-03        | CP-31 | CP-060106 | 1114 | 1   | IMS AKA - content of initial authentication header                                    | 7.2.0 | 7.3.0 | C1-060450 |  |
| 2006-03        | CP-31 | CP-060106 | 1204 | -   | Syntax and operation for Security-Client, Security-Server and Security-Verify headers | 7.2.0 | 7.3.0 | C1-060387 |  |
| 2006-03        | CP-31 | CP-060107 | 1148 | 1   | UE processing 305 (Use Proxy)   | 7.2.0 | 7.3.0 | C1-060507 |  |
| 2006-03        | CP-31 | CP-060107 | 1164 | 1   | Clarifications on P-CSCF discovery  | 7.2.0 | 7.3.0 | C1-060459 |  |
| 2006-03        | CP-31 | CP-060107 | 1161 | 1   | DHCPv6 options for Domain Name Servers  | 7.2.0 | 7.3.0 | C1-060456 |  |
| 2006-03        | CP-31 | CP-060110 | 1136 | 1   | SDP answer  | 7.2.0 | 7.3.0 | C1-060472 |  |
| 2006-03        | CP-31 | CP-060110 | 1206 | -   | Inclusion of Ma reference point   | 7.2.0 | 7.3.0 | C1-060392 |  |
| 2006-03        | CP-31 | CP-060110 | 1134 | -   | Preconditions required  | 7.2.0 | 7.3.0 | C1-060192 |  |
| 2006-03        | CP-31 | CP-060110 | 1156 | 1   | Tables Change in Appendix A   | 7.2.0 | 7.3.0 | C1-060478 |  |
| 2006-03        | CP-31 | CP-060110 | 1132 | 1   | P-Asserted-Identity   | 7.2.0 | 7.3.0 | C1-060476 |  |
| 2006-03        | CP-31 | CP-060111 | 1219 | -   | Reference Update of TS24.229, Rel7  | 7.2.0 | 7.3.0 | C1-060483 |  |
| 2006-03        | CP-31 | CP-060111 | 1119 | 2   | IMS Short Session Setup - Clarifications  | 7.2.0 | 7.3.0 | C1-060595 |  |
| 2006-03        | CP-31 | CP-060111 | 1189 | 3   | Definition of principles for IOI exchange and storage                                 | 7.2.0 | 7.3.0 | C1-060610 |  |
| 2006-03        | CP-31 | CP-060111 | 1129 | 2   | Tel URI   | 7.2.0 | 7.3.0 | C1-060593 |  |
| 2006-03        | CP-31 | CP-060117 | 1210 | 1   | Coding of P-Access-Network-Info header for 3GPP2 IMS                                  | 7.2.0 | 7.3.0 | C1-060494 |  |
| 2006-03        | CP-31 | CP-060118 | 1103 | 1   | Editor's Note on xDSL bearer  | 7.2.0 | 7.3.0 | C1-060119 |  |
| 2006-03        | CP-31 | CP-060118 | 1095 | 1   | Reference to new annexes on NAT   | 7.2.0 | 7.3.0 | C1-060116 |  |
| 2006-03        | CP-31 | CP-060118 | 1101 | -   | Replaces header in Profile Tables   | 7.2.0 | 7.3.0 | C1-060051 |  |
| 2006-03        | CP-31 | CP-060118 | 1093 | 2   | P-Access-Network-Info header absence for emergency call detection                     | 7.2.0 | 7.3.0 | C1-060339 |  |
| 2006-03        | CP-31 | CP-060118 | 1196 | 1   | correction for the procedure of changing media data                                   | 7.2.0 | 7.3.0 | C1-060518 |  |
| 2006-03        | CP-31 | CP-060118 | 1197 | 1   | Editorial Changes   | 7.2.0 | 7.3.0 | C1-060519 |  |
| 2006-03        | CP-31 | CP-060118 | 1092 | 3   | Optionality of P-Access-Network-Info header   | 7.2.0 | 7.3.0 | C1-060338 |  |



| Change history |       |           |      |     |   |       |       |           |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2006-03        | CP-31 | CP-060118 | 1086 | 1   | Addition of TISPAN supported internet-drafts  | 7.2.0 | 7.3.0 | C1-060337 |
| 2006-03        | CP-31 | CP-060118 | 1089 | 1   | IBCF corrections  | 7.2.0 | 7.3.0 | C1-060110 |
| 2006-03        | CP-31 | CP-060118 | 1106 | 4   | Completion of IBCF routing procedures   | 7.2.0 | 7.3.0 | C1-060498 |
| 2006-03        | CP-31 | CP-060118 | 1088 | 4   | IBCF enhancements   | 7.2.0 | 7.3.0 | C1-060603 |
| 2006-03        | CP-31 | CP-060119 | 1177 | 1   | PacketCable Extensions to P-Charging-Vector header  | 7.2.0 | 7.3.0 | C1-060512 |
| 2006-03        | CP-31 | CP-060120 | 1098 | 4   | Emergency service S-CSCF impact   | 7.2.0 | 7.3.0 | C1-060601 |
| 2006-03        | CP-31 | CP-060120 | 1097 | 5   | Emergency service - P-CSCF impact   | 7.2.0 | 7.3.0 | C1-060600 |
| 2006-03        | CP-31 | CP-060120 | 1099 | 5   | Emergency service - E-CSCF impact   | 7.2.0 | 7.3.0 | C1-060599 |
| 2006-03        | CP-31 | CP-060120 | 1096 | 5   | Emergency service - UE impact   | 7.2.0 | 7.3.0 | C1-060602 |
| 2006-03        | CP-31 | CP-060121 | 1183 | -   | Transfer of Text from the Combinational Services TR 24.879 to TS 24.229   | 7.2.0 | 7.3.0 | C1-060311 |
| 2006-03        | CP-31 | CP-060124 | 1138 | 2   | Session termination by P-CSCF   | 7.2.0 | 7.3.0 | C1-060605 |
| 2006-03        | CP-31 | CP-060124 | 1157 | 3   | Support for RFC 4145  | 7.2.0 | 7.3.0 | C1-060621 |
| 2006-03        | CP-31 | CP-060124 | 1184 | 3   | Registration of multiple PUIs - CR  | 7.2.0 | 7.3.0 | C1-060608 |
| 2006-03        | CP-31 | CP-060124 | 1137 | 1   | Session termination by S-CSCF   | 7.2.0 | 7.3.0 | C1-060533 |
| 2006-03        | CP-31 | CP-060124 | 1152 | 1   | Editorial Changes   | 7.2.0 | 7.3.0 | C1-060539 |
| 2006-03        | CP-31 | CP-060124 | 1107 | 1   | Reference Update of TS24.229  | 7.2.0 | 7.3.0 | C1-060123 |
| 2006-03        | CP-31 | CP-060124 | 1125 | -   | Pre-loaded Route header   | 7.2.0 | 7.3.0 | C1-060183 |
| 2006-03        | CP-31 | CP-060142 | 1226 | 1   | Transport of HSS address from I-CSCF to S-CSCF  | 7.2.0 | 7.3.0 | -         |
| 2006-03        | CP-31 | CP-060153 | 1222 | 2   | Mandation of RFC 4320 fixes for issues found with the Session Initiation Protocol's (SIP) Non-INVITE Transactions | 7.2.0 | 7.3.0 | -         |
| 2006-03        | CP-31 | CP-060176 | 1225 | 2   | Support of call forwarding at the S-CSCF  | 7.2.0 | 7.3.0 | -         |
| 2006-06        | CP-32 | CP-060232 | 1290 | 2   | Realm Parameter Handling  | 7.3.0 | 7.4.0 |           |
| 2006-06        | CP-32 | CP-060249 | 1242 | 3   | SDP answer  | 7.3.0 | 7.4.0 |           |
| 2006-06        | CP-32 | CP-060262 | 1309 | 2   | Hiding correction   | 7.3.0 | 7.4.0 | C1-061115 |
| 2006-06        | CP-32 | CP-060262 | 1306 | 2   | 3rd-party registration  | 7.3.0 | 7.4.0 | C1-061098 |
| 2006-06        | CP-32 | CP-060262 | 1303 | 1   | One private identity one contact  | 7.3.0 | 7.4.0 | C1-061095 |
| 2006-06        | CP-32 | CP-060264 | 1274 | 2   | Re-authentication during deregistration   | 7.3.0 | 7.4.0 | C1-061113 |
| 2006-06        | CP-32 | CP-060265 | 1312 |     | I-CSCF registration procedure correction  | 7.3.0 | 7.4.0 | C1-060829 |
| 2006-06        | CP-32 | CP-060266 | 1265 | 1   | IOI overview  | 7.3.0 | 7.4.0 | C1-060997 |
| 2006-06        | CP-32 | CP-060266 | 1271 | 1   | Introduction of signalling encryption   | 7.3.0 | 7.4.0 | C1-060999 |
| 2006-06        | CP-32 | CP-060266 | 1348 |     | UE behavior after timer F expiry  | 7.3.0 | 7.4.0 | C1-060897 |
| 2006-06        | CP-32 | CP-060266 | 1236 | 2   | P-Asserted-ID   | 7.3.0 | 7.4.0 | C1-061119 |
| 2006-06        | CP-32 | CP-060266 | 1238 | 1   | Via header in the initial registration  | 7.3.0 | 7.4.0 | C1-060975 |
| 2006-06        | CP-32 | CP-060266 | 1327 | 1   | Incorrect requirement on I-CSCF   | 7.3.0 | 7.4.0 | C1-061079 |
| 2006-06        | CP-32 | CP-060270 | 1247 | 1   | Emergency PUID  | 7.3.0 | 7.4.0 | C1-061054 |

| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2006-06        | CP-32 | CP-060270 | 1266 | 1   | Inclusion of draft-ietf-ecrit-service-urn                                    | 7.3.0 | 7.4.0 | C1-061009 |
| 2006-06        | CP-32 | CP-060270 | 1229 |     | Emergency service S-CSCF impact  | 7.3.0 | 7.4.0 | C1-060642 |
| 2006-06        | CP-32 | CP-060270 | 1360 |     | Inclusion of E-CSCF in subclause 3.1 and subclause 4.1                       | 7.3.0 | 7.4.0 | C1-060923 |
| 2006-06        | CP-32 | CP-060270 | 1249 | 2   | Emergency call release   | 7.3.0 | 7.4.0 | C1-061121 |
| 2006-06        | CP-32 | CP-060270 | 1338 | 1   | Adding RDF in E-CSCF procedure   | 7.3.0 | 7.4.0 | C1-061060 |
| 2006-06        | CP-32 | CP-060270 | 1358 | 1   | Priority handling for emergency calls at the E-CSCF                          | 7.3.0 | 7.4.0 | C1-061017 |
| 2006-06        | CP-32 | CP-060270 | 1357 | 1   | Priority handling for emergency calls at the S-CSCF                          | 7.3.0 | 7.4.0 | C1-061015 |
| 2006-06        | CP-32 | CP-060270 | 1356 | 1   | Priority handling for emergency calls at the P-CSCF                          | 7.3.0 | 7.4.0 | C1-061013 |
| 2006-06        | CP-32 | CP-060270 | 1354 |     | Inclusion of session timer procedures at the E-CSCF                          | 7.3.0 | 7.4.0 | C1-060917 |
| 2006-06        | CP-32 | CP-060270 | 1340 | 2   | TEL URI associated with emergency IMPU                                       | 7.3.0 | 7.4.0 | C1-061120 |
| 2006-06        | CP-32 | CP-060270 | 1337 | 1   | Getting local emergency numbers  | 7.3.0 | 7.4.0 | C1-061010 |
| 2006-06        | CP-32 | CP-060270 | 1336 | 1   | Some corrections in IMS emergency calls                                      | 7.3.0 | 7.4.0 | C1-061059 |
| 2006-06        | CP-32 | CP-060271 | 1258 | 1   | UDP encapsulation of IPsec   | 7.3.0 | 7.4.0 | C1-061019 |
| 2006-06        | CP-32 | CP-060271 | 1318 | 1   | Extensions to P-Access-Network-Info header for DOCSIS Access                 | 7.3.0 | 7.4.0 | C1-061025 |
| 2006-06        | CP-32 | CP-060271 | 1317 | 2   | PRACK  | 7.3.0 | 7.4.0 | C1-061026 |
| 2006-06        | CP-32 | CP-060271 | 1267 | 1   | IBCF corrections   | 7.3.0 | 7.4.0 | C1-061022 |
| 2006-06        | CP-32 | CP-060271 | 1259 | 1   | IBCF initiated call release  | 7.3.0 | 7.4.0 | C1-061021 |
| 2006-06        | CP-32 | CP-060271 | 1345 | 1   | Correction of the reference document   | 7.3.0 | 7.4.0 | C1-061082 |
| 2006-06        | CP-32 | CP-060274 | 1234 | 1   | Final NOTIFY   | 7.3.0 | 7.4.0 | C1-060989 |
| 2006-06        | CP-32 | CP-060274 | 1255 |     | Full notification  | 7.3.0 | 7.4.0 | C1-060686 |
| 2006-06        | CP-32 | CP-060274 | 1260 |     | Reg event package parameters in notification                                 | 7.3.0 | 7.4.0 | C1-060704 |
| 2006-06        | CP-32 | CP-060274 | 1261 |     | Subscription refreshing  | 7.3.0 | 7.4.0 | C1-060705 |
| 2006-06        | CP-32 | CP-060274 | 1217 | 2   | Definition of B2BUA  | 7.3.0 | 7.4.0 | C1-061074 |
| 2006-06        | CP-32 | CP-060274 | 1277 | 1   | Usage of associated public user identities                                   | 7.3.0 | 7.4.0 | C1-060964 |
| 2006-06        | CP-32 | CP-060274 | 1321 |     | Verification by I-CSCF of trust domain origin for incoming requests          | 7.3.0 | 7.4.0 | C1-060844 |
| 2006-06        | CP-32 | CP-060274 | 1322 |     | Miscellaneous Correction   | 7.3.0 | 7.4.0 | C1-060845 |
| 2006-06        | CP-32 | CP-060274 | 1328 | 1   | Resilience to registration and authentication errors                         | 7.3.0 | 7.4.0 | C1-061080 |
| 2006-06        | CP-32 | CP-060274 | 1335 | 1   | The Correction on the description for the information of registration status | 7.3.0 | 7.4.0 | C1-060986 |
| 2006-06        | CP-32 | CP-060274 | 1361 |     | Reference updates  | 7.3.0 | 7.4.0 | C1-060924 |
| 2006-06        | CP-32 | CP-060283 | 1366 |     | Emergency service – UE impact  | 7.3.0 | 7.4.0 |           |
| 2006-06        | CP-32 | CP-060284 | 1367 |     | Emergency service- E-CSCF impact   | 7.3.0 | 7.4.0 |           |
| 2006-06        | CP-32 | CP-060335 | 1232 | 3   | Handling of P-Charging-Addresses   | 7.3.0 | 7.4.0 |           |
| 2006-06        | CP-32 | CP-060345 | 1365 | 1   | Registration of several unrelated public user identities                     | 7.3.0 | 7.4.0 |           |

| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2006-06        | CP-32 | CP-060352 | 1228 | 4   | Emergency service P-CSCF-impact  | 7.3.0 | 7.4.0 | C1-061134 |
| 2006-09        | CP-33 | CP-060452 | 1461 | 1   | Correction of Realm Parameter Handling for S-CSCF procedures             | 7.4.0 | 7.5.0 | C1-061732 |
| 2006-09        | CP-33 | CP-060452 | 1467 |     | SDP reference revision   | 7.4.0 | 7.5.0 | C1-061657 |
| 2006-09        | CP-33 | CP-060452 | 1475 | 2   | "Response" value in unprotected Register requests                        | 7.4.0 | 7.5.0 | C1-061845 |
| 2006-09        | CP-33 | CP-060463 | 1351 | 3   | Treatment of emergency requests other than INVITE requests at the P-CSCF | 7.4.0 | 7.5.0 | C1-061357 |
| 2006-09        | CP-33 | CP-060463 | 1352 | 3   | Treatment of emergency requests other than INVITE requests at the E-CSCF | 7.4.0 | 7.5.0 | C1-061358 |
| 2006-09        | CP-33 | CP-060463 | 1369 | 1   | UE emergency deregistration  | 7.4.0 | 7.5.0 | C1-061304 |
| 2006-09        | CP-33 | CP-060463 | 1370 | 1   | Emergency subscription   | 7.4.0 | 7.5.0 | C1-061305 |
| 2006-09        | CP-33 | CP-060463 | 1371 | 1   | P-CSCF emergency subscription  | 7.4.0 | 7.5.0 | C1-061306 |
| 2006-09        | CP-33 | CP-060463 | 1373 | 2   | S-CSCF emergency registration  | 7.4.0 | 7.5.0 | C1-061350 |
| 2006-09        | CP-33 | CP-060463 | 1374 | 2   | Handling of Emergency registration in S-CSCF                             | 7.4.0 | 7.5.0 | C1-061349 |
| 2006-09        | CP-33 | CP-060463 | 1375 | 2   | Handling of emergency registration at the UE                             | 7.4.0 | 7.5.0 | C1-061351 |
| 2006-09        | CP-33 | CP-060463 | 1379 | 4   | Location handling E-CSCF   | 7.4.0 | 7.5.0 | C1-061913 |
| 2006-09        | CP-33 | CP-060463 | 1380 | 1   | Clarification of Emergency Session Setup without prior IMS Registration  | 7.4.0 | 7.5.0 | C1-061311 |
| 2006-09        | CP-33 | CP-060463 | 1381 | 1   | Clarifications to subclause 5.1.6.1                                      | 7.4.0 | 7.5.0 | C1-061313 |
| 2006-09        | CP-33 | CP-060463 | 1383 | 1   | Non-INVITE requests  | 7.4.0 | 7.5.0 | C1-061314 |
| 2006-09        | CP-33 | CP-060463 | 1384 | 2   | IP-CAN for emergency calls   | 7.4.0 | 7.5.0 | C1-061355 |
| 2006-09        | CP-33 | CP-060463 | 1390 | 1   | Adoption of terminology from draft-ietf-ecrit-requirements               | 7.4.0 | 7.5.0 | C1-061315 |
| 2006-09        | CP-33 | CP-060463 | 1391 | 3   | Minor corrections to EMC1 text from previous CRs                         | 7.4.0 | 7.5.0 | C1-061367 |
| 2006-09        | CP-33 | CP-060463 | 1414 | 2   | Handling of location information at E-CSCF                               | 7.4.0 | 7.5.0 | C1-061860 |
| 2006-09        | CP-33 | CP-060463 | 1440 | 2   | P-Asserted-Identity in P-CSCF handling                                   | 7.4.0 | 7.5.0 | C1-061861 |
| 2006-09        | CP-33 | CP-060463 | 1443 | 4   | Handling of PSAP address mapping result at E-CSCF                        | 7.4.0 | 7.5.0 | C1-061919 |
| 2006-09        | CP-33 | CP-060465 | 1413 | 1   | Miscellaneous Corrections in Annex F                                     | 7.4.0 | 7.5.0 | C1-061826 |
| 2006-09        | CP-33 | CP-060465 | 1420 | 1   | Transit IMS  | 7.4.0 | 7.5.0 | C1-061827 |
| 2006-09        | CP-33 | CP-060465 | 1425 | 1   | P-CSCF procedures for session release when QoS resources are unavailable | 7.4.0 | 7.5.0 | C1-061830 |
| 2006-09        | CP-33 | CP-060465 | 1427 | 1   | Make SDP bandwidth modifiers optional for standard RTCP usage            | 7.4.0 | 7.5.0 | C1-061832 |
| 2006-09        | CP-33 | CP-060465 | 1430 | 3   | Addition of the cpc parameter to TS24.229                                | 7.4.0 | 7.5.0 | C1-061882 |
| 2006-09        | CP-33 | CP-060466 | 1385 | 4   | Introduction of GRUU in 24.229   | 7.4.0 | 7.5.0 | C1-061858 |
| 2006-09        | CP-33 | CP-060466 | 1386 | 5   | S-SCSF procedures to support GRUU  | 7.4.0 | 7.5.0 | C1-061915 |
| 2006-09        | CP-33 | CP-060468 | 1405 |     | Original dialog identifier   | 7.4.0 | 7.5.0 | C1-061408 |
| 2006-09        | CP-33 | CP-060468 | 1406 |     | No-fork  | 7.4.0 | 7.5.0 | C1-061409 |
| 2006-09        | CP-33 | CP-060468 | 1409 |     | Connection address - zero  | 7.4.0 | 7.5.0 | C1-061412 |

| Change history |       |           |      |     |   |       |       |           |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2006-09        | CP-33 | CP-060468 | 1415 |     | Reference for populating the "Anonymous" From header  | 7.4.0 | 7.5.0 | C1-061439 |
| 2006-09        | CP-33 | CP-060468 | 1439 | 1   | Usage of P-Associated-URI   | 7.4.0 | 7.5.0 | C1-061759 |
| 2006-09        | CP-33 | CP-060468 | 1450 |     | Clarification of network initiated deregistration to match reginfo format   | 7.4.0 | 7.5.0 | C1-061585 |
| 2006-09        | CP-33 | CP-060468 | 1456 | 2   | Authentication between UA and UA  | 7.4.0 | 7.5.0 | C1-061851 |
| 2006-09        | CP-33 | CP-060468 | 1457 | 2   | Treatment by S-CSCF of profile changes for registered PUIs  | 7.4.0 | 7.5.0 | C1-061853 |
| 2006-09        | CP-33 | CP-060468 | 1458 | 1   | Completion of RFC 4320 fixes for 100 Trying responses Non-INVITE Transactions RFC 4320 fixes for 100 Trying responses Non-INVITE Transactions tration | 7.4.0 | 7.5.0 | C1-061765 |
| 2006-09        | CP-33 | CP-060468 | 1463 |     | Correction to S-CSCF procedures for UE-originated requests  | 7.4.0 | 7.5.0 | C1-061646 |
| 2006-09        | CP-33 | CP-060468 | 1464 | 1   | SCTP transport  | 7.4.0 | 7.5.0 | C1-061766 |
| 2006-09        | CP-33 | CP-060504 | 1257 | 4   | SDP usage at MGCF   | 7.4.0 | 7.5.0 | C1-061847 |
| 2006-09        | CP-33 | CP-060504 | 1417 | 1   | Type 3 orig-ioi in I-CSCF   | 7.4.0 | 7.5.0 | C1-061744 |
| 2006-09        | CP-33 | CP-060504 | 1469 |     | SDP corrections   | 7.4.0 | 7.5.0 | C1-061659 |
| 2006-09        | CP-33 | CP-060504 | 1471 |     | SDP completion  | 7.4.0 | 7.5.0 | C1-061661 |
| 2006-09        | CP-33 | CP-060504 | 1478 | 1   | Updates to Profile Tables UE Major Capabilities   | 7.4.0 | 7.5.0 | C1-061754 |
| 2006-09        | CP-33 | CP-060504 | 1481 |     | Removal of Editor's notes in 24.229, rel-6  | 7.4.0 | 7.5.0 | C1-061745 |
| 2006-09        | CP-33 | CP-060504 | 1483 |     | Final codec selection   | 7.4.0 | 7.5.0 | C1-061850 |
| 2006-09        | CP-33 | CP-060526 | 1418 | 3   | Originating requests on behalf of an unregistered user  | 7.4.0 | 7.5.0 | C1-061758 |
| 2006-09        |       |           |      |     | Version 7.5.1 created by MCC to correct styles  | 7.5.0 | 7.5.1 |           |
| 2006-12        | CP-34 | CP-060655 | 1502 | -   | RFC reference update  | 7.5.1 | 7.6.0 | C1-061977 |
| 2006-12        | CP-34 | CP-060655 | 1506 | -   | SDP group attribute correction  | 7.5.1 | 7.6.0 | C1-061981 |
| 2006-12        | CP-34 | CP-060655 | 1504 | 1   | Addressing editor's notes relating to trust domains   | 7.5.1 | 7.6.0 | C1-062304 |
| 2006-12        | CP-34 | CP-060655 | 1546 | -   | Join header correction  | 7.5.1 | 7.6.0 | C1-062205 |
| 2006-12        | CP-34 | CP-060655 | 1508 | 2   | Processing the successful response at S-CSCF  | 7.5.1 | 7.6.0 | C1-062434 |
| 2006-12        | CP-34 | CP-060655 | 1449 | 2   | Correction of S-CSCF construction and UE interpretation of registration event notification  | 7.5.1 | 7.6.0 | C1-062317 |
| 2006-12        | CP-34 | CP-060655 | 1514 | 1   | Removal of more Editor's notes in 24.229, rel-6   | 7.5.1 | 7.6.0 | C1-062310 |
| 2006-12        | CP-34 | CP-060659 | 1491 | 2   | Location handling for emergency   | 7.5.1 | 7.6.0 | C1-062437 |
| 2006-12        | CP-34 | CP-060659 | 1521 | 1   | Location information for IMS emergency  | 7.5.1 | 7.6.0 | C1-062293 |
| 2006-12        | CP-34 | CP-060659 | 1529 | 2   | Emergency re-registration due to mobility   | 7.5.1 | 7.6.0 | C1-062436 |
| 2006-12        | CP-34 | CP-060659 | 1515 | 1   | Removal of Editor's notes on emergency call in clause 4   | 7.5.1 | 7.6.0 | C1-062292 |
| 2006-12        | CP-34 | CP-060659 | 1484 | 1   | Corrections to emergency call procedures for P-Asserted-Identity header   | 7.5.1 | 7.6.0 | C1-062289 |
| 2006-12        | CP-34 | CP-060659 | 1543 | -   | Next hop is the BGCF  | 7.5.1 | 7.6.0 | C1-062181 |
| 2006-12        | CP-34 | CP-060659 | 1536 | -   | Editorial corrections to emergency call text  | 7.5.1 | 7.6.0 | C1-062142 |

| Change history |       |           |      |     |   |       |       |           |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2006-12        | CP-34 | CP-060659 | 1542 | 1   | minor correction to EMC of UE and PCSCF                                 | 7.5.1 | 7.6.0 | C1-062299 |
| 2006-12        | CP-34 | CP-060659 | 1490 | 2   | Emergency call on existing registration                                 | 7.5.1 | 7.6.0 | C1-062435 |
| 2006-12        | CP-34 | CP-060660 | 1486 | 2   | Introduction of communication service concept in TS 24229               | 7.5.1 | 7.6.0 | C1-062451 |
| 2006-12        | CP-34 | CP-060662 | 1494 | 1   | Tel URI translation   | 7.5.1 | 7.6.0 | C1-062325 |
| 2006-12        | CP-34 | CP-060662 | 1523 | 1   | I-CSCF procedure  | 7.5.1 | 7.6.0 | C1-062333 |
| 2006-12        | CP-34 | CP-060662 | 1544 | -   | Clarification of UEs initial SDP offer                                  | 7.5.1 | 7.6.0 | C1-062189 |
| 2006-12        | CP-34 | CP-060662 | 1493 | 1   | Alias URI   | 7.5.1 | 7.6.0 | C1-062324 |
| 2006-12        | CP-34 | CP-060662 | 1525 | 1   | Clarification of iFC execution for UE-terminated requests at S-CSCF     | 7.5.1 | 7.6.0 | C1-062334 |
| 2006-12        | CP-34 | CP-060662 | 1533 | 1   | SIP response code to unknown method                                     | 7.5.1 | 7.6.0 | C1-062336 |
| 2006-12        | CP-34 | CP-060662 | 1537 | -   | Originating requests on behalf of an unregistered user                  | 7.5.1 | 7.6.0 | C1-062143 |
| 2006-12        | CP-34 | CP-060662 | 1538 | -   | Treatment by S-CSCF of profile changes for registered PUIs              | 7.5.1 | 7.6.0 | C1-062144 |
| 2006-12        | CP-34 | CP-060662 | 1547 | -   | Corrections to Profile table for RFC 4320 compliance                    | 7.5.1 | 7.6.0 | C1-062210 |
| 2006-12        | CP-34 | CP-060662 | 1539 | -   | Miscellaneous editorial corrections                                     | 7.5.1 | 7.6.0 | C1-062145 |
| 2006-12        | CP-34 | CP-060662 | 1509 | 1   | No-forking at AS  | 7.5.1 | 7.6.0 | C1-062329 |
| 2006-12        | CP-34 | CP-060662 | 1528 | 2   | P-Visited-Network-ID on ISC interface                                   | 7.5.1 | 7.6.0 | C1-062442 |
| 2006-12        | CP-34 | CP-060662 | 1487 | 1   | Introduction of P-Profile Key in TS 24.229                              | 7.5.1 | 7.6.0 | C1-062322 |
| 2006-12        | CP-34 | CP-060662 | 1522 | 1   | Local numbering   | 7.5.1 | 7.6.0 | C1-062338 |
| 2006-12        | CP-34 | CP-060662 | 1495 | 2   | BGCF procedures   | 7.5.1 | 7.6.0 | C1-062440 |
| 2006-12        | CP-34 | CP-060662 | 1498 | 2   | AS acting as PSI  | 7.5.1 | 7.6.0 | C1-062441 |
| 2006-12        | CP-34 | CP-060662 | 1524 | -   | Clarification of the URI in UE-terminating requests at the P-CSCF       | 7.5.1 | 7.6.0 | C1-062061 |
| 2006-12        | CP-34 | CP-060662 | 1549 | 1   | Core Network Service Authorizatrion                                     | 7.5.1 | 7.6.0 | C1-062339 |
| 2006-12        | CP-34 | CP-060663 | 1527 | 3   | Align with GRUU IETF draft 11   | 7.5.1 | 7.6.0 | C1-062512 |
| 2006-12        | CP-34 | CP-060663 | 1496 | 1   | I-CSCF processing GRUU  | 7.5.1 | 7.6.0 | C1-062340 |
| 2006-12        | CP-34 | CP-060663 | 1497 | 1   | S-CSCF processing GRUU  | 7.5.1 | 7.6.0 | C1-062341 |
| 2006-12        | CP-34 | CP-060663 | 1422 | 3   | GRUU processing by non-UE User Agents                                   | 7.5.1 | 7.6.0 | C1-062343 |
| 2006-12        | CP-34 | CP-060667 | 1426 | 3   | Allowing an asserted display name to be conveyed with a Public Identity | 7.5.1 | 7.6.0 | C1-062427 |
| 2006-12        | CP-34 | CP-060667 | 1429 | 4   | Update to NAT Traversal procedures in support of Outbound and ICE       | 7.5.1 | 7.6.0 | C1-062515 |
| 2006-12        | CP-34 | CP-060667 | 1540 | 2   | Annex I (Transit IMS) improvements                                      | 7.5.1 | 7.6.0 | C1-062516 |
| 2007-03        | CP-35 | CP-070130 | 1566 | -   | Session Establishment Interworking with Rel-5 UEs                       | 7.6.0 | 7.7.0 | C1-070052 |
| 2007-03        | CP-35 | CP-070130 | 1638 | -   | Inclusion of draft-ietf-sip-uri-list-message in SIP profile             | 7.6.0 | 7.7.0 | C1-070266 |
| 2007-03        | CP-35 | CP-070130 | 1619 | -   | Clarifications on resource reservation                                  | 7.6.0 | 7.7.0 | C1-070180 |
| 2007-03        | CP-35 | CP-070130 | 1621 | 1   | Routeing B2BUA handling of Replaces header                              | 7.6.0 | 7.7.0 | C1-070439 |

| Change history |       |           |      |     |   |       |       |           |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2007-03        | CP-35 | CP-070132 | 1609 | -   | Establishing an emergency session   | 7.6.0 | 7.7.0 | C1-070147 |
| 2007-03        | CP-35 | CP-070132 | 1575 | -   | Deletion of editors note in subclause 5.1.6.5   | 7.6.0 | 7.7.0 | C1-070068 |
| 2007-03        | CP-35 | CP-070132 | 1639 | -   | Identification of emergency calls   | 7.6.0 | 7.7.0 | C1-070276 |
| 2007-03        | CP-35 | CP-070132 | 1593 | 1   | Limitation on Emergency Registration  | 7.6.0 | 7.7.0 | C1-070424 |
| 2007-03        | CP-35 | CP-070132 | 1586 | 1   | Tidyup UE clause  | 7.6.0 | 7.7.0 | C1-070418 |
| 2007-03        | CP-35 | CP-070132 | 1654 | 1   | Double reference removal  | 7.6.0 | 7.7.0 | C1-070381 |
| 2007-03        | CP-35 | CP-070132 | 1605 | 1   | Emergency PUID  | 7.6.0 | 7.7.0 | C1-070419 |
| 2007-03        | CP-35 | CP-070132 | 1569 | 1   | Handling of parallel emergency registration   | 7.6.0 | 7.7.0 | C1-070413 |
| 2007-03        | CP-35 | CP-070132 | 1574 | 1   | Deletion of editors note in subclause 5.1.6.2   | 7.6.0 | 7.7.0 | C1-070414 |
| 2007-03        | CP-35 | CP-070132 | 1568 | 1   | Connecting to an Emergency APN  | 7.6.0 | 7.7.0 | C1-070409 |
| 2007-03        | CP-35 | CP-070132 | 1581 | 1   | Deletion of Editor' s notes in 5.2.10   | 7.6.0 | 7.7.0 | C1-070416 |
| 2007-03        | CP-35 | CP-070132 | 1641 | -   | Correction of service-urn   | 7.6.0 | 7.7.0 | C1-070278 |
| 2007-03        | CP-35 | CP-070132 | 1589 | -   | Correction of CR#1484r1 implementation error (subclause 5.1.6.8.3)                                    | 7.6.0 | 7.7.0 | C1-070111 |
| 2007-03        | CP-35 | CP-070132 | 1610 | -   | Emergency session-no registration   | 7.6.0 | 7.7.0 | C1-070148 |
| 2007-03        | CP-35 | CP-070134 | 1612 | 2   | Emergency treatment at P-CSCF   | 7.6.0 | 7.7.0 | C1-070563 |
| 2007-03        | CP-35 | CP-070134 | 1635 | 1   | Remove the term ESRP  | 7.6.0 | 7.7.0 | C1-070430 |
| 2007-03        | CP-35 | CP-070134 | 1607 | 2   | Emergency call at P-CSCF  | 7.6.0 | 7.7.0 | C1-070443 |
| 2007-03        | CP-35 | CP-070134 | 1632 | 1   | Backward compatibility for using 380 response   | 7.6.0 | 7.7.0 | C1-070429 |
| 2007-03        | CP-35 | CP-070134 | 1653 | 3   | Location for emergency  | 7.6.0 | 7.7.0 | C1-070618 |
| 2007-03        | CP-35 | CP-070134 | 1626 | 1   | Handling of re-registration when user redial emergency number   | 7.6.0 | 7.7.0 | C1-070426 |
| 2007-03        | CP-35 | CP-070134 | 1582 | 2   | Deletion of editors notes in 5.11 and 5.4.8   | 7.6.0 | 7.7.0 | C1-070615 |
| 2007-03        | CP-35 | CP-070134 | 1567 | 3   | Home Network Indication for Emergency Calls   | 7.6.0 | 7.7.0 | C1-070640 |
| 2007-03        | CP-35 | CP-070134 | 1631 | 2   | Correction to emergency call procedure with non-emergency registration for P-Asserted-Identity header | 7.6.0 | 7.7.0 | C1-070617 |
| 2007-03        | CP-35 | CP-070137 | 1634 | 1   | Profile definition for CSI application server   | 7.6.0 | 7.7.0 | C1-070469 |
| 2007-03        | CP-35 | CP-070138 | 1660 | 1   | Format of dsl-location  | 7.6.0 | 7.7.0 | C1-070552 |
| 2007-03        | CP-35 | CP-070138 | 1595 | 1   | Deletion of EN's in clause 5.10   | 7.6.0 | 7.7.0 | C1-070547 |
| 2007-03        | CP-35 | CP-070138 | 1594 | -   | Deletion of EN's in Annex G   | 7.6.0 | 7.7.0 | C1-070132 |
| 2007-03        | CP-35 | CP-070139 | 1613 | 2   | Annex K NAT Traversal Procedural and References Updates   | 7.6.0 | 7.7.0 | C1-070626 |
| 2007-03        | CP-35 | CP-070139 | 1617 | 1   | Routing of SIP URI "user=phone" when domain doesn't own target user                                   | 7.6.0 | 7.7.0 | C1-070551 |
| 2007-03        | CP-35 | CP-070139 | 1614 | 1   | Annex A updates for Annex K NAT Traversal Procedurals   | 7.6.0 | 7.7.0 | C1-070550 |
| 2007-03        | CP-35 | CP-070140 | 1598 | 1   | Forked MESSAGE request  | 7.6.0 | 7.7.0 | C1-070451 |
| 2007-03        | CP-35 | CP-070140 | 1558 | 1   | Removal of notes for screening functionality  | 7.6.0 | 7.7.0 | C1-070441 |

| Change history |       |           |      |     |   |       |       |           |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2007-03        | CP-35 | CP-070140 | 1556 | 1   | Handling of special characters in the local service number  | 7.6.0 | 7.7.0 | C1-070458 |
| 2007-03        | CP-35 | CP-070140 | 1655 | 2   | Forwarding a request by transit functions in the S-CSCF   | 7.6.0 | 7.7.0 | C1-070586 |
| 2007-03        | CP-35 | CP-070140 | 1587 | 1   | Terminating case in S-CSCF  | 7.6.0 | 7.7.0 | C1-070449 |
| 2007-03        | CP-35 | CP-070140 | 1559 | -   | Completion of SIP timers functionality  | 7.6.0 | 7.7.0 | C1-070039 |
| 2007-03        | CP-35 | CP-070140 | 1588 | 1   | P-User-Database   | 7.6.0 | 7.7.0 | C1-070450 |
| 2007-03        | CP-35 | CP-070140 | 1560 | 1   | Removal of notes for SIGCOMP functionality  | 7.6.0 | 7.7.0 | C1-070442 |
| 2007-03        | CP-35 | CP-070140 | 1557 | -   | Removal of normative statements in NOTES  | 7.6.0 | 7.7.0 | C1-070037 |
| 2007-03        | CP-35 | CP-070140 | 1604 | 1   | Forwarding P-Charging-Vector outside the home network   | 7.6.0 | 7.7.0 | C1-070453 |
| 2007-03        | CP-35 | CP-070140 | 1555 | 1   | Removal of Editor's notes for message bodies  | 7.6.0 | 7.7.0 | C1-070440 |
| 2007-03        | CP-35 | CP-070140 | 1652 | -   | Correction for local numbers  | 7.6.0 | 7.7.0 | C1-070341 |
| 2007-03        | CP-35 | CP-070140 | 1601 | -   | Tel URI translation   | 7.6.0 | 7.7.0 | C1-070139 |
| 2007-03        | CP-35 | CP-070140 | 1646 | 1   | Align definition of Alias URI with the description in 23.228  | 7.6.0 | 7.7.0 | C1-070455 |
| 2007-03        | CP-35 | CP-070140 | 1600 | 2   | Dual IP addresses   | 7.6.0 | 7.7.0 | C1-070584 |
| 2007-03        | CP-35 | CP-070142 | 1642 | -   | SIP extensions covering URI-lists   | 7.6.0 | 7.7.0 | C1-070279 |
| 2007-03        | CP-35 | CP-070148 | 1564 | 1   | Network Initiated / Modified Media PDP Contexts   | 7.6.0 | 7.7.0 | C1-070447 |
| 2007-03        | CP-35 | CP-070149 | 1643 | -   | SDP usage in association with BFCP (additions to SDP profile)   | 7.6.0 | 7.7.0 | C1-070282 |
| 2007-03        | CP-35 | CP-070151 | 1648 | 2   | S-CSCF inserts P-Called-Party-ID before forwarding request towards served user  | 7.6.0 | 7.7.0 | C1-070588 |
| 2007-03        | CP-35 | CP-070151 | 1597 | 1   | Instance ID   | 7.6.0 | 7.7.0 | C1-070461 |
| 2007-03        | CP-35 | CP-070151 | 1615 | 1   | Signalling Public User Identity to AS when request URI is Temp-GRUU   | 7.6.0 | 7.7.0 | C1-070463 |
| 2007-03        | CP-35 | CP-070214 | 1640 | 3   | Location conveyance revisions   | 7.6.0 | 7.7.0 |           |
| 2007-03        | CP-35 | CP-070242 | 1576 | 3   | Deletion of editors notes in subclauses 5.1.6.8.2, 5.1.6.8.3, 5.1.6.8.4   | 7.6.0 | 7.7.0 |           |
| 2007-03        | CP-35 | CP-070252 | 1658 | 4   | Profile for IBCF  | 7.6.0 | 7.7.0 |           |
| 2007-03        | CP-35 | CP-070254 | 1580 | 3   | PCC introduction to TS 24.229   | 7.6.0 | 7.7.0 |           |
| 2007-03        | CP-35 | CP-070255 | 1630 | 3   | Corrections for the handling of target refresh requests at the S-CSCF   | 7.6.0 | 7.7.0 |           |
| 2007-03        | CP-35 | CP-070271 | 1623 | 5   | Further alignment with phonebcp draft   | 7.6.0 | 7.7.0 |           |
| 2007-06        | CP-36 | CP-070370 | 1749 | 1   | Correction of coding rules of P-Access-Network-Info header  | 7.7.0 | 7.8.0 | C1-071435 |
| 2007-06        | CP-36 | CP-070370 | 1689 | 2   | Inclusion of "addressing an amplification vulnerability in session initiation protocol forking proxies" (draft-ietf-sip-fork-loop-fix) in the SIP profile | 7.7.0 | 7.8.0 | C1-071409 |
| 2007-06        | CP-36 | CP-070373 | 1666 | 2   | Protocol between E-CSCF and LRF   | 7.7.0 | 7.8.0 | C1-071040 |
| 2007-06        | CP-36 | CP-070373 | 1690 | -   | Further alignment with phonebcp draft   | 7.7.0 | 7.8.0 | C1-070779 |
| 2007-06        | CP-36 | CP-070373 | 1763 | 1   | Emergency registration clarification  | 7.7.0 | 7.8.0 | C1-071441 |

| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2007-06        | CP-36 | CP-070373 | 1665 | 1   | Definition of identities used for emergency call   | 7.7.0 | 7.8.0 | C1-070957 |
| 2007-06        | CP-36 | CP-070374 | 1714 | 1   | Alignment of layout of access technology specific annexes  | 7.7.0 | 7.8.0 | C1-071032 |
| 2007-06        | CP-36 | CP-070374 | 1715 | 1   | GPRS IP-CAN change of normative requirement out of scope to informative  | 7.7.0 | 7.8.0 | C1-071033 |
| 2007-06        | CP-36 | CP-070374 | 1732 | 2   | Clarification on iFC execution   | 7.7.0 | 7.8.0 | C1-071460 |
| 2007-06        | CP-36 | CP-070374 | 1721 | 1   | UE un-subscribing to reg-event   | 7.7.0 | 7.8.0 | C1-071419 |
| 2007-06        | CP-36 | CP-070374 | 1722 | -   | MO Record-Route at P-CSCF  | 7.7.0 | 7.8.0 | C1-071051 |
| 2007-06        | CP-36 | CP-070374 | 1723 | 1   | MT Record-Route at P-CSCF  | 7.7.0 | 7.8.0 | C1-071420 |
| 2007-06        | CP-36 | CP-070374 | 1727 | 1   | Double registration  | 7.7.0 | 7.8.0 | C1-071422 |
| 2007-06        | CP-36 | CP-070374 | 1730 | 1   | Inclusion of new mandatory elements of SigComp   | 7.7.0 | 7.8.0 | C1-071423 |
| 2007-06        | CP-36 | CP-070374 | 1731 | 1   | Use of a presence specific dictionary in SigComp   | 7.7.0 | 7.8.0 | C1-071424 |
| 2007-06        | CP-36 | CP-070374 | 1720 | 1   | Registration and deregistration  | 7.7.0 | 7.8.0 | C1-071418 |
| 2007-06        | CP-36 | CP-070374 | 1746 | 1   | Correction to P-CSCF procedures for cancellation of a session currently being established  | 7.7.0 | 7.8.0 | C1-071431 |
| 2007-06        | CP-36 | CP-070374 | 1762 | 1   | Originating a terminating request in an AS   | 7.7.0 | 7.8.0 | C1-071433 |
| 2007-06        | CP-36 | CP-070374 | 1769 | 2   | Clarification to Original Dialog Identifier  | 7.7.0 | 7.8.0 | C1-071463 |
| 2007-06        | CP-36 | CP-070374 | 1761 | -   | Local numbering clarification  | 7.7.0 | 7.8.0 | C1-071196 |
| 2007-06        | CP-36 | CP-070374 | 1760 | 1   | PANI related corrections   | 7.7.0 | 7.8.0 | C1-071437 |
| 2007-06        | CP-36 | CP-070374 | 1743 | 1   | The precondition mechanism may be required in subsequent SDP offer/answer exchanges  | 7.7.0 | 7.8.0 | C1-071430 |
| 2007-06        | CP-36 | CP-070374 | 1772 | -   | Minor miscellaneous clean-up   | 7.7.0 | 7.8.0 | C1-071231 |
| 2007-06        | CP-36 | CP-070374 | 1739 | 1   | P-CSCF processing of P-Early-Media   | 7.7.0 | 7.8.0 | C1-071428 |
| 2007-06        | CP-36 | CP-070374 | 1738 | 3   | Originating UE sending of P-Early-Media  | 7.7.0 | 7.8.0 | C1-071462 |
| 2007-06        | CP-36 | CP-070374 | 1737 | 2   | Originating UE processing of P-Early-Media   | 7.7.0 | 7.8.0 | C1-071461 |
| 2007-06        | CP-36 | CP-070375 | 1692 | -   | Profile support for a session initiation protocol event package and data format for various settings in support for the push-to-talk over cellular service (RFC4354)                               | 7.7.0 | 7.8.0 | C1-070781 |
| 2007-06        | CP-36 | CP-070375 | 1562 | 4   | Completion of Phone-context parameter in rel-7   | 7.7.0 | 7.8.0 | C1-071009 |
| 2007-06        | CP-36 | CP-070375 | 1700 | -   | Translation of non-international format numbers  | 7.7.0 | 7.8.0 | C1-070810 |
| 2007-06        | CP-36 | CP-070375 | 1680 | -   | Outgoing Request URI=pres or IM URI processing clarification and misc clean-up   | 7.7.0 | 7.8.0 | C1-070705 |
| 2007-06        | CP-36 | CP-070375 | 1691 | 1   | Profile support for the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular (draft-allen-sipping-poc-p-answer-state-header) | 7.7.0 | 7.8.0 | C1-070987 |
| 2007-06        | CP-36 | CP-070375 | 1678 | 1   | Qvalue   | 7.7.0 | 7.8.0 | C1-070984 |
| 2007-06        | CP-36 | CP-070375 | 1704 | -   | Minor miscellaneous clean-up   | 7.7.0 | 7.8.0 | C1-070824 |
| 2007-06        | CP-36 | CP-070375 | 1703 | -   | Filter criteria evaluation when the AS changes the P-Asserted-Identity   | 7.7.0 | 7.8.0 | C1-070823 |
| 2007-06        | CP-36 | CP-070378 | 1718 | 1   | Addition to network initiated PDP context  | 7.7.0 | 7.8.0 | C1-071346 |



| Change history |       |           |      |     |   |       |       |           |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2007-06        | CP-36 | CP-070380 | 1679 | -   | Cleanup of Signalling Public GRUU to AS   | 7.7.0 | 7.8.0 | C1-070704 |
| 2007-06        | CP-36 | CP-070380 | 1663 | -   | Provide GRUU functionality in case of hosted NAT  | 7.7.0 | 7.8.0 | C1-070663 |
| 2007-06        | CP-36 | CP-070380 | 1756 | 1   | GRUU Alignment with stage 2   | 7.7.0 | 7.8.0 | C1-071456 |
| 2007-06        | CP-36 | CP-070380 | 1686 | 2   | Alternate GRUU for AS acting on behalf of Public User Identity  | 7.7.0 | 7.8.0 | C1-071010 |
| 2007-06        | CP-36 | CP-070380 | 1713 | 2   | Cleanup of GRUU   | 7.7.0 | 7.8.0 | C1-071238 |
| 2007-06        | CP-36 | CP-070380 | 1766 | 1   | Management of GRUU  | 7.7.0 | 7.8.0 | C1-071457 |
| 2007-06        | CP-36 | CP-070380 | 1711 | 2   | Use of GRUU for Emergency Sessions  | 7.7.0 | 7.8.0 | C1-071458 |
| 2007-06        | CP-36 | CP-070383 | 1773 | -   | IMS Communication Service ID registration   | 7.7.0 | 7.8.0 | C1-071234 |
| 2007-06        | CP-36 | CP-070383 | 1645 | 6   | IMS Communication Service ID 24.229   | 7.7.0 | 7.8.0 | C1-071475 |
| 2007-06        | CP-36 | CP-070388 | 1735 | 2   | Correction on the handling of CPC parameter regarding trust domain  | 7.7.0 | 7.8.0 | C1-071464 |
| 2007-06        | CP-36 | CP-070388 | 1662 | -   | Tidyup open issues from FBI work item   | 7.7.0 | 7.8.0 | C1-070662 |
| 2007-06        | CP-36 | CP-070388 | 1596 | 5   | Update to NAT Traversal procedures in support of Outbound and ICE   | 7.7.0 | 7.8.0 | C1-071400 |
| 2007-06        | CP-36 | CP-070388 | 1740 | 1   | IBCF processing of P-Early-Media  | 7.7.0 | 7.8.0 | C1-071404 |
| 2007-06        | CP-36 | CP-070388 | 1742 | 1   | IBCF Path header  | 7.7.0 | 7.8.0 | C1-071405 |
| 2007-06        | CP-36 | CP-070436 | 1696 | 3   | Endorsement of P-Early-Media header draft   | 7.7.0 | 7.8.0 |           |
| 2007-06        | CP-36 | CP-070447 | 1698 | 3   | Report of new transit scenario documented in stage 2  | 7.7.0 | 7.8.0 | -         |
| 2007-06        | CP-36 | CP-070450 | 1771 | 3   | THIG processing correction to ensure conformity to RFC 3261   | 7.7.0 | 7.8.0 | -         |
| 2007-06        | CP-36 | CP-070496 | 1717 | 4   | PCC impact  | 7.7.0 | 7.8.0 | -         |
| 2007-06        | CP-36 | CP-070393 | 1751 | 1   | Resource-Priority header and trust domains  | 7.7.0 | 8.0.0 | C1-071446 |
| 2007-06        | CP-36 | CP-070393 | 1695 | 2   | Inclusion policy for Resource-Priority header in support of multimedia priority service                                   | 7.7.0 | 8.0.0 | C1-071443 |
| 2007-06        | CP-36 | CP-070393 | 1694 | 2   | Inclusion of "communications resource priority for the session initiation protocol" (RFC4412) in the SIP profile          | 7.7.0 | 8.0.0 | C1-071444 |
| 2007-06        | CP-36 | CP-070393 | 1693 | 1   | Inclusion of "extending the session initiation protocol Reason header for preemption events" (RFC4411) in the SIP profile | 7.7.0 | 8.0.0 | C1-070918 |
| 2007-06        | CP-36 | CP-070396 | 1682 | 2   | IMS Enhancements to Support Number Portability (NP) for Cable Networks  | 7.7.0 | 8.0.0 | C1-070994 |
| 2007-06        | CP-36 | CP-070396 | 1681 | 4   | Enhancements to Support Preferred Circuit Carrier Access and Dial-Around for Cable Networks                               | 7.7.0 | 8.0.0 | C1-071294 |
| 2007-09        | CP-37 | CP-070578 | 1945 |     | Correction of the Authorization Header in the Profile Table   | 8.0.0 | 8.1.0 | C1-072085 |
| 2007-09        | CP-37 | CP-070578 | 1811 |     | Integrity param in De- and ReREGISTER   | 8.0.0 | 8.1.0 | C1-071573 |
| 2007-09        | CP-37 | CP-070579 | 1905 | 2   | Clarification of DTD  | 8.0.0 | 8.1.0 | C1-072150 |
| 2007-09        | CP-37 | CP-070580 | 1795 | 2   | Unprotected registration at UE  | 8.0.0 | 8.1.0 | C1-072153 |
| 2007-09        | CP-37 | CP-070580 | 1876 |     | IETF reference updates  | 8.0.0 | 8.1.0 | C1-071772 |
| 2007-09        | CP-37 | CP-070580 | 1924 | 1   | P-Access-Network-Info header clarification  | 8.0.0 | 8.1.0 | C1-072042 |

| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2007-09        | CP-37 | CP-070580 | 1922 | 1   | Optional rport parameter in UE   | 8.0.0 | 8.1.0 | C1-072039 |
| 2007-09        | CP-37 | CP-070580 | 1797 | 1   | Unprotected registration at S-CSCF   | 8.0.0 | 8.1.0 | C1-072052 |
| 2007-09        | CP-37 | CP-070584 | 1866 |     | Emergency Registration without eAPN  | 8.0.0 | 8.1.0 | C1-071728 |
| 2007-09        | CP-37 | CP-070585 | 1878 |     | IETF reference updates relating to emergency call feature  | 8.0.0 | 8.1.0 | C1-071776 |
| 2007-09        | CP-37 | CP-070585 | 1892 | 1   | Correction of emergency procedures unregistered user case  | 8.0.0 | 8.1.0 | C1-072018 |
| 2007-09        | CP-37 | CP-070585 | 1894 |     | Emergency registration timer in visited network  | 8.0.0 | 8.1.0 | C1-071808 |
| 2007-09        | CP-37 | CP-070585 | 1927 |     | Contents of From header when initiating an emergency session within a emergency registration             | 8.0.0 | 8.1.0 | C1-071874 |
| 2007-09        | CP-37 | CP-070586 | 1861 | 1   | Correction for the URNs of IMS Communication Service Identifier and IMS Application Reference Identifier | 8.0.0 | 8.1.0 | C1-071956 |
| 2007-09        | CP-37 | CP-070586 | 1909 | 2   | Completing UE ICSI/IARI procedures   | 8.0.0 | 8.1.0 | C1-072162 |
| 2007-09        | CP-37 | CP-070586 | 1842 | 1   | S-CSCF option to add P-Asserted-Service in UE-originated case  | 8.0.0 | 8.1.0 | C1-071952 |
| 2007-09        | CP-37 | CP-070586 | 1911 | 2   | Completing S-CSCF ICSI/IARI procedures   | 8.0.0 | 8.1.0 | C1-072164 |
| 2007-09        | CP-37 | CP-070586 | 1826 | 1   | Cleanup of text related to contact header dealing with ICSI  | 8.0.0 | 8.1.0 | C1-071942 |
| 2007-09        | CP-37 | CP-070586 | 1838 | 2   | Description of the ICSI as an assigned identifier  | 8.0.0 | 8.1.0 | C1-072159 |
| 2007-09        | CP-37 | CP-070586 | 1929 | 1   | ICSI Alignments with reqs 2, 3 and 11  | 8.0.0 | 8.1.0 | C1-071947 |
| 2007-09        | CP-37 | CP-070586 | 1942 | 1   | UE usage of ServidID received from the network   | 8.0.0 | 8.1.0 | C1-072181 |
| 2007-09        | CP-37 | CP-070586 | 1840 |     | Correction of application server handling of ICSI and IARI values  | 8.0.0 | 8.1.0 | C1-071676 |
| 2007-09        | CP-37 | CP-070590 | 1807 | 3   | Trust Domain in IMS  | 8.0.0 | 8.1.0 | C1-072185 |
| 2007-09        | CP-37 | CP-070590 | 1799 | 1   | Unprotected registration at P-CSCF   | 8.0.0 | 8.1.0 | C1-072054 |
| 2007-09        | CP-37 | CP-070590 | 1793 | 1   | Protected registration   | 8.0.0 | 8.1.0 | C1-072046 |
| 2007-09        | CP-37 | CP-070590 | 1804 | 1   | No multiple simultaneous Registration  | 8.0.0 | 8.1.0 | C1-072056 |
| 2007-09        | CP-37 | CP-070590 | 1864 | 1   | Corrections of tables in Annex A   | 8.0.0 | 8.1.0 | C1-072065 |
| 2007-09        | CP-37 | CP-070590 | 1879 | 1   | Essential corrections to P-Early-Media header procedures   | 8.0.0 | 8.1.0 | C1-072062 |
| 2007-09        | CP-37 | CP-070590 | 1881 |     | IETF SigComp reference updates   | 8.0.0 | 8.1.0 | C1-071779 |
| 2007-09        | CP-37 | CP-070590 | 1934 |     | SIP related reference update   | 8.0.0 | 8.1.0 | C1-071888 |
| 2007-09        | CP-37 | CP-070590 | 1913 | 1   | Removal of IBCF Route Headers Editors Note   | 8.0.0 | 8.1.0 | C1-072073 |
| 2007-09        | CP-37 | CP-070590 | 1854 | 1   | Clarification on P-Profile-Key   | 8.0.0 | 8.1.0 | C1-072063 |
| 2007-09        | CP-37 | CP-070592 | 1817 |     | Resolve FFS for AS-GRUU  | 8.0.0 | 8.1.0 | C1-071581 |
| 2007-09        | CP-37 | CP-070596 | 1885 | 2   | Update Emergency NAT Traversal Procedures Annex K  | 8.0.0 | 8.1.0 | C1-072078 |
| 2007-09        | CP-37 | CP-070596 | 1883 | 1   | Update GRUU NAT Traversal Procedures Annex-K   | 8.0.0 | 8.1.0 | C1-071926 |
| 2007-09        | CP-37 | CP-070600 | 1750 | 3   | Resource-Priority and priority   | 7.8.0 | 8.1.0 | C1-072132 |
| 2007-09        | CP-37 | CP-070600 | 1919 | 2   | Addition of MGCF for optional support of Resource-Priority   | 8.0.0 | 8.1.0 | C1-072184 |

| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2007-09        | CP-37 | CP-070601 | 1815 | 2   | Updates to Annex K in support of SIP Digest and TLS procedures   | 8.0.0 | 8.1.0 | C1-072137 |
| 2007-09        | CP-37 | CP-070601 | 1812 | 4   | UE Digest and TLS Procedures   | 8.0.0 | 8.1.0 | C1-072172 |
| 2007-09        | CP-37 | CP-070601 | 1814 | 4   | S-CSCF Digest and TLS Procedures   | 8.0.0 | 8.1.0 | C1-072174 |
| 2007-09        | CP-37 | CP-070601 | 1813 | 4   | P-CSCF Digest and TLS Procedures   | 8.0.0 | 8.1.0 | C1-072173 |
| 2007-09        | CP-37 | CP-070603 | 1847 | 1   | Cleanup of SigComp dictionary support  | 8.0.0 | 8.1.0 | C1-072144 |
| 2007-09        | CP-37 | CP-070603 | 1896 | 1   | S-CSCF procedure corrections   | 8.0.0 | 8.1.0 | C1-072089 |
| 2007-09        | CP-37 | CP-070603 | 1935 |     | Restructuring of subclause 5.2.6 (General treatment for all dialogs and standalone transactions excluding the REGISTER method) of the P-CSCF | 8.0.0 | 8.1.0 | C1-071891 |
| 2007-09        | CP-37 | CP-070603 | 1788 | 2   | Request-URI in registration  | 8.0.0 | 8.1.0 | C1-072154 |
| 2007-09        | CP-37 | CP-070670 | 1907 | 3   | Definition of feature tag for IARI/ICSI  | 8.0.0 | 8.1.0 | C1-072006 |
| 2007-09        | CP-37 | CP-070674 | 1791 | 2   | Emergency registration   | 8.0.0 | 8.1.0 | C1-072016 |
| 2007-09        | CP-37 | CP-070676 | 1851 | 4   | P-CSCF behaviour upon loss of SIP signalling transport   | 8.0.0 | 8.1.0 | C1-072178 |
| 2007-09        | CP-37 | CP-070691 | 1926 | 5   | UE setting of IARI   | 8.0.0 | 8.1.0 | C1-072166 |
| 2007-12        | CP-38 | CP-070735 | 2077 | 1   | Update P-Early-Media Reference   | 8.1.0 | 8.2.0 | C1-072750 |
| 2007-12        | CP-38 | CP-070785 | 2065 |     | Authenticating with AKAv1-MD5  | 8.1.0 | 8.2.0 | C1-072533 |
| 2007-12        | CP-38 | CP-070785 | 2115 |     | Proxy profile corrections  | 8.1.0 | 8.2.0 | C1-072922 |
| 2007-12        | CP-38 | CP-070785 | 2111 |     | Corrections to RFC 3329 entries in profile   | 8.1.0 | 8.2.0 | C1-072918 |
| 2007-12        | CP-38 | CP-070785 | 2041 | 1   | Corrections for re-authenticating user   | 8.1.0 | 8.2.0 | C1-072553 |
| 2007-12        | CP-38 | CP-070785 | 2049 | 3   | Introduction of versioning and conventions   | 8.1.0 | 8.2.0 | C1-072989 |
| 2007-12        | CP-38 | CP-070788 | 2028 | 1   | Coverage of access technology specific text  | 8.1.0 | 8.2.0 | C1-072746 |
| 2007-12        | CP-38 | CP-070788 | 2017 | 2   | Action on missing "integrity-protected" parameter  | 8.1.0 | 8.2.0 | C1-073179 |
| 2007-12        | CP-38 | CP-070788 | 2035 | 1   | MGCF does not act as a proxy   | 8.1.0 | 8.2.0 | C1-072565 |
| 2007-12        | CP-38 | CP-070788 | 2070 | 1   | Correction to subclause 7.2A.5.2.2   | 8.1.0 | 8.2.0 | C1-073052 |
| 2007-12        | CP-38 | CP-070791 | 1999 | 1   | 380 at normal call setup   | 8.1.0 | 8.2.0 | C1-072670 |
| 2007-12        | CP-38 | CP-070791 | 2062 | 2   | Miscellaneous EMC1 corrections   | 8.1.0 | 8.2.0 | C1-072748 |
| 2007-12        | CP-38 | CP-070791 | 2120 |     | Introductory text for emergency service  | 8.1.0 | 8.2.0 | C1-072930 |
| 2007-12        | CP-38 | CP-070794 | 1990 |     | Correct sub-section references in Annex-K  | 8.1.0 | 8.2.0 | C1-072295 |
| 2007-12        | CP-38 | CP-070794 | 2023 |     | Correction of outbound and ice option tag support in profile tables  | 8.1.0 | 8.2.0 | C1-072383 |
| 2007-12        | CP-38 | CP-070795 | 1986 | 1   | Align with draft-gruu-reg-ev-09  | 8.1.0 | 8.2.0 | C1-072752 |
| 2007-12        | CP-38 | CP-070795 | 2043 | 1   | Addition of GRUU to emergency set-up when registration exists  | 8.1.0 | 8.2.0 | C1-072599 |
| 2007-12        | CP-38 | CP-070799 | 2067 | 1   | P-CSCF Releases/Rejects session due to PCRF responses  | 8.1.0 | 8.2.0 | C1-073067 |
| 2007-12        | CP-38 | CP-070805 | 2053 | 2   | Terminating UE ICSI procedures   | 8.1.0 | 8.2.0 | C1-072708 |
| 2007-12        | CP-38 | CP-070805 | 2021 | 1   | Correction to digest and TLS Procedures for Annex K  | 8.1.0 | 8.2.0 | C1-072508 |

| Change history |       |           |      |     |   |       |       |           |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2007-12        | CP-38 | CP-070805 | 1951 | 1   | Correction to the examples for ICSI and IARI values                                   | 8.1.0 | 8.2.0 | C1-072490 |
| 2007-12        | CP-38 | CP-070805 | 2014 | 2   | Encoding of ICSI and IARI within the g.ims.app_ref feature tag                        | 8.1.0 | 8.2.0 | C1-072704 |
| 2007-12        | CP-38 | CP-070805 | 2051 | 1   | Multiple IARI/ICSI values in g.ims.app_ref feature tag                                | 8.1.0 | 8.2.0 | C1-072512 |
| 2007-12        | CP-38 | CP-070805 | 1969 | 1   | One ICSI value per P-Preferred-Service header   | 8.0.0 | 8.2.0 | C1-072496 |
| 2007-12        | CP-38 | CP-070805 | 1963 | 1   | Change of name for feature tag g.ims.app_ref  | 8.0.0 | 8.2.0 | C1-072492 |
| 2007-12        | CP-38 | CP-070806 | 2008 | 2   | Handling of invalid and unauthorized media based on Communication Service Identifiers | 8.1.0 | 8.2.0 | C1-072702 |
| 2007-12        | CP-38 | CP-070806 | 2092 | 2   | S-CSCF Processing of P-Preferred-Service and P-Asserted-Service                       | 8.1.0 | 8.2.0 | C1-073204 |
| 2007-12        | CP-38 | CP-070806 | 2107 | 2   | The received list of ICSIs from the Network   | 8.1.0 | 8.2.0 | C1-073206 |
| 2007-12        | CP-38 | CP-070806 | 2088 |     | ICSI in Annex F   | 8.1.0 | 8.2.0 | C1-072841 |
| 2007-12        | CP-38 | CP-070806 | 2019 | 2   | Miscellaneous service identifier corrections  | 8.1.0 | 8.2.0 | C1-073106 |
| 2007-12        | CP-38 | CP-070806 | 1965 | 3   | Minor corrections to P-Preferred and P-Asserted Service headers                       | 8.1.0 | 8.2.0 | C1-073102 |
| 2007-12        | CP-38 | CP-070806 | 1976 | 2   | Correction to S-CSCF handling of IMS communication service                            | 8.1.0 | 8.2.0 | C1-072700 |
| 2007-12        | CP-38 | CP-070807 | 2005 | 1   | No SIPS   | 8.1.0 | 8.2.0 | C1-072593 |
| 2007-12        | CP-38 | CP-070807 | 1961 | 1   | Route header verification at P-CSCF   | 8.1.0 | 8.2.0 | C1-072587 |
| 2007-12        | CP-38 | CP-070807 | 1955 | 1   | Update of the reference for P-Profile-Key Private Header (P-Header)                   | 8.1.0 | 8.2.0 | C1-072487 |
| 2007-12        | CP-38 | CP-070807 | 2012 |     | Reference alignment   | 8.1.0 | 8.2.0 | C1-072364 |
| 2007-12        | CP-38 | CP-070807 | 2037 | 1   | AS does not subscribe to reg-event package when user is unregistered                  | 8.1.0 | 8.2.0 | C1-072597 |
| 2007-12        | CP-38 | CP-070807 | 2045 | 2   | Correction of mutually exclusive ICSI and GRUU  | 8.1.0 | 8.2.0 | C1-072706 |
| 2007-12        | CP-38 | CP-070807 | 2055 |     | Update of P-Answer-State header draft Reference                                       | 8.1.0 | 8.2.0 | C1-072446 |
| 2007-12        | CP-38 | CP-070808 | 2057 | 2   | Clarification of UE handling of the P-Early-Media header.                             | 8.1.0 | 8.2.0 | C1-072723 |
| 2007-12        | CP-38 | CP-070808 | 2100 | 1   | Access Network Info for I-WLAN  | 8.1.0 | 8.2.0 | C1-073075 |
| 2007-12        | CP-38 | CP-070808 | 2003 | 2   | Service Profile Change  | 8.1.0 | 8.2.0 | C1-072718 |
| 2007-12        | CP-38 | CP-070808 | 1957 | 4   | Correction to the IBCF subsection in relation with trusted domain                     | 8.1.0 | 8.2.0 | C1-072687 |
| 2007-12        | CP-38 | CP-070808 | 2072 | 2   | Correction to procedure when registration timer times out                             | 8.1.0 | 8.2.0 | C1-073173 |
| 2007-12        | CP-38 | CP-070808 | 2103 | 1   | Access Network Info for 3GPP2/UMB   | 8.1.0 | 8.2.0 | C1-073057 |
| 2007-12        | CP-38 | CP-070810 | 2081 | 3   | Correction of multiple Contact headers in abnormal case                               | 8.1.0 | 8.2.0 | C1-073226 |
| 2007-12        | CP-38 | CP-070810 | 2117 | 1   | Miscellaneous editorial corrections (part 3)  | 8.1.0 | 8.2.0 | C1-073165 |
| 2007-12        | CP-38 | CP-070810 | 1932 | 4   | Incorporation of draft-ietf-consent-framework   | 8.1.0 | 8.2.0 | C1-073166 |
| 2007-12        | CP-38 | CP-070810 | 2098 | 1   | Superfluous requirements for removing charging information at terminating P-CSCF      | 8.1.0 | 8.2.0 | C1-073164 |

| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2007-12        | CP-38 | CP-070810 | 1974 | 1   | Synchronization When Service Profile Being Modified  | 8.1.0 | 8.2.0 | C1-072661 |
| 2007-12        | CP-38 | CP-070810 | 2029 | 3   | Miscellaneous editorial corrections  | 8.1.0 | 8.2.0 | C1-072764 |
| 2007-12        | CP-38 | CP-070810 | 2059 | 3   | Miscellaneous editorial corrections (part 2)   | 8.1.0 | 8.2.0 | C1-073162 |
| 2007-12        | CP-38 | CP-070811 | 2078 | 1   | Clarification on interconnect functionalities  | 8.1.0 | 8.2.0 | C1-073163 |
| 2007-12        | CP-38 | CP-070812 | 2086 | 1   | Semantics for values in "integrity-protected" field  | 8.1.0 | 8.2.0 | C1-073112 |
| 2007-12        | CP-38 | CP-070812 | 2060 | 3   | Public user identity and private user identity derivation in UEs without UICC              | 8.1.0 | 8.2.0 | C1-073201 |
| 2007-12        | CP-38 | CP-070812 | 2006 | 1   | Digest Support in Profile Tables   | 8.1.0 | 8.2.0 | C1-072623 |
| 2007-12        | CP-38 | CP-070812 | 2026 | 1   | Security-related references and definitions  | 8.1.0 | 8.2.0 | C1-072761 |
| 2007-12        | CP-38 | CP-070812 | 2025 | 3   | Introduction to security mechanisms  | 8.1.0 | 8.2.0 | C1-073175 |
| 2007-12        | CP-38 | CP-070812 | 1982 | 6   | Updates to integrity protection for digest and TLS   | 8.1.0 | 8.2.0 | C1-073202 |
| 2007-12        | CP-38 | CP-070814 | 2085 | 4   | Addition of SIP header to support UUS1   | 8.1.0 | 8.2.0 | C1-073208 |
| 2007-12        | CP-38 | CP-070816 | 2024 | 5   | Integration of text for digest and TLS plus digest into the main body of the specification | 8.1.0 | 8.2.0 | C1-073200 |
| 2007-12        | CP-38 | CP-070864 | 1953 | 5   | Clarifications on NW-init and resource reservation   | 8.1.0 | 8.2.0 | C1-073069 |
| 2007-12        | CP-38 | CP-070875 | 1997 | 4   | Corrections for emergency procedures   | 8.1.0 | 8.2.0 | C1-072991 |
| 2008-03        | CP-39 | CP-080120 | 2174 |     | Reference correction for RFC 4244  | 8.2.0 | 8.3.0 | C1-080147 |
| 2008-03        | CP-39 | CP-080120 | 2149 |     | Handling of the reason header in requests at the MGCF                                      | 8.2.0 | 8.3.0 | C1-080045 |
| 2008-03        | CP-39 | CP-080120 | 2162 | 1   | Correction on handling of P-Charging-Vector at IBCF  | 8.2.0 | 8.3.0 | C1-080515 |
| 2008-03        | CP-39 | CP-080120 | 2181 | 1   | Correction of Alias  | 8.2.0 | 8.3.0 | C1-080517 |
| 2008-03        | CP-39 | CP-080120 | 2176 |     | SDP with precondition  | 8.2.0 | 8.3.0 | C1-080149 |
| 2008-03        | CP-39 | CP-080126 | 2201 | 2   | Handling of Service ID in interworking cases   | 8.2.0 | 8.3.0 | C1-080630 |
| 2008-03        | CP-39 | CP-080126 | 2155 | 2   | Clarification on the use of IARI in the contact header                                     | 8.2.0 | 8.3.0 | C1-080635 |
| 2008-03        | CP-39 | CP-080126 | 2183 | 2   | UE behaviour when no ICSI is contained in the Accept-Contact header                        | 8.2.0 | 8.3.0 | C1-080531 |
| 2008-03        | CP-39 | CP-080130 | 2143 | 1   | Procedure at S-CSCF  | 8.2.0 | 8.3.0 | C1-080600 |
| 2008-03        | CP-39 | CP-080130 | 2144 |     | Empty RES  | 8.2.0 | 8.3.0 | C1-080009 |
| 2008-03        | CP-39 | CP-080130 | 2145 | 1   | Alias URI  | 8.2.0 | 8.3.0 | C1-080601 |
| 2008-03        | CP-39 | CP-080130 | 2146 | 2   | Notification at S-CSCF   | 8.2.0 | 8.3.0 | C1-080631 |
| 2008-03        | CP-39 | CP-080130 | 2156 | 1   | Correction of example of IARI coding   | 8.2.0 | 8.3.0 | C1-080526 |
| 2008-03        | CP-39 | CP-080130 | 2160 | 1   | Correction on the value used for P-Preferred-Identity header at UE                         | 8.2.0 | 8.3.0 | C1-080513 |
| 2008-03        | CP-39 | CP-080130 | 2170 | 1   | Correction to user initiated emergency re-registration                                     | 8.2.0 | 8.3.0 | C1-080405 |
| 2008-03        | CP-39 | CP-080130 | 2187 | 1   | IPv4 and IPv6 support  | 8.2.0 | 8.3.0 | C1-080609 |
| 2008-03        | CP-39 | CP-080130 | 2188 | 4   | P-CSCF awareness for 3GPP accesses   | 8.2.0 | 8.3.0 | C1-080658 |
| 2008-03        | CP-39 | CP-080130 | 2196 | 2   | Annex K: ICE procedures for the IBCF   | 8.2.0 | 8.3.0 | C1-080643 |

| Change history |       |           |      |     |   |       |       |           |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2008-03        | CP-39 | CP-080131 | 2192 | 1   | Completion of CIC and DAI requirements for MGCF                   | 8.2.0 | 8.3.0 | C1-080472 |
| 2008-03        | CP-39 | CP-080132 | 2163 | 1   | Miscelanous Corrections on SIP Digest                             | 8.2.0 | 8.3.0 | C1-080473 |
| 2008-03        | CP-39 | CP-080132 | 2189 | 1   | Enhancements to security introduction text                        | 8.2.0 | 8.3.0 | C1-080474 |
| 2008-03        | CP-39 | CP-080134 | 2190 | 1   | Inclusion of NASS bundled authentication                          | 8.2.0 | 8.3.0 | C1-080518 |
| 2008-03        | CP-39 | CP-080139 | 2164 | 1   | SIP XML addition for support of transit specific content          | 8.2.0 | 8.3.0 | C1-080533 |
| 2008-03        | CP-39 | CP-080140 | 2138 | 2   | IP-CAN procedure for cdma2000                                     | 8.2.0 | 8.3.0 | C1-080411 |
| 2008-03        | CP-39 | CP-080140 | 2141 | 2   | P-CSCF interface to IP-CAN  | 8.2.0 | 8.3.0 | C1-080413 |
| 2008-03        | CP-39 | CP-080140 | 2140 | 2   | Access-network-charging-info for cdma2000 access                  | 8.2.0 | 8.3.0 | C1-080412 |
| 2008-03        | CP-39 | CP-080141 | 2197 | 1   | Wildcarded Public User Identity: P-CSCF impact                    | 8.2.0 | 8.3.0 | C1-080612 |
| 2008-03        | CP-39 | CP-080141 | 2198 | 2   | Wildcarded Public User Identity: S-CSCF impact                    | 8.2.0 | 8.3.0 | C1-080644 |
| 2008-03        | CP-39 | CP-080199 | 2147 | 4   | NAT traversal   | 8.2.0 | 8.3.0 |           |
| 2008-03        | CP-39 | CP-080201 | 2151 | 5   | Handling of the reason header in responses                        | 8.2.0 | 8.3.0 |           |
| 2008-06        | CP-40 | CP-080338 | 2288 | 1   | Correction to de-registration procedure when registration expired | 8.3.0 | 8.4.0 | C1-081936 |
| 2008-06        | CP-40 | CP-080340 | 2215 | -   | Revision of references to documents from IETF ECRIT working group | 8.3.0 | 8.4.0 | C1-080854 |
| 2008-06        | CP-40 | CP-080341 | 2243 | 1   | Correction to P-CSCF session release procedures                   | 8.3.0 | 8.4.0 | C1-081336 |
| 2008-06        | CP-40 | CP-080341 | 2275 | 2   | Addition of AVPF support  | 8.3.0 | 8.4.0 | C1-082022 |
| 2008-06        | CP-40 | CP-080341 | 2258 | 1   | Correction on identifiers distinguishing the dialog               | 8.3.0 | 8.4.0 | C1-081338 |
| 2008-06        | CP-40 | CP-080341 | 2238 | 1   | Removal of reason header annex                                    | 8.3.0 | 8.4.0 | C1-081334 |
| 2008-06        | CP-40 | CP-080341 | 2217 | -   | Revision of references to documents from IETF                     | 8.3.0 | 8.4.0 | C1-080858 |
| 2008-06        | CP-40 | CP-080341 | 2277 | 1   | Addition of the SDP Capability Negotiaion mechanism               | 8.3.0 | 8.4.0 | C1-081932 |
| 2008-06        | CP-40 | CP-080343 | 2158 | 6   | Handling of SDP at the terminating UE                             | 8.3.0 | 8.4.0 | C1-082050 |
| 2008-06        | CP-40 | CP-080344 | 2290 | -   | Correction of GRUU references                                     | 8.3.0 | 8.4.0 | C1-081799 |
| 2008-06        | CP-40 | CP-080349 | 2236 | -   | Revision of references to documents from IETF SIP working group   | 8.3.0 | 8.4.0 | C1-080860 |
| 2008-06        | CP-40 | CP-080353 | 2203 | 1   | Emergency calls - NAT traversal at UE                             | 8.3.0 | 8.4.0 | C1-081228 |
| 2008-06        | CP-40 | CP-080353 | 2204 | 1   | NAT traversal for emergency calls at P-CSCF                       | 8.3.0 | 8.4.0 | C1-081229 |
| 2008-06        | CP-40 | CP-080353 | 2220 | 1   | PANI header text revision   | 8.3.0 | 8.4.0 | C1-081346 |
| 2008-06        | CP-40 | CP-080353 | 2225 | 1   | Addition of 802.11n to P-Access-Network-Info header               | 8.3.0 | 8.4.0 | C1-081348 |
| 2008-06        | CP-40 | CP-080353 | 2205 | 3   | "im" URI  | 8.3.0 | 8.4.0 | C1-081411 |
| 2008-06        | CP-40 | CP-080353 | 2254 | 2   | Annex K: Moving of IBCF ICE procedures                            | 8.3.0 | 8.4.0 | C1-081469 |
| 2008-06        | CP-40 | CP-080353 | 2168 | 9   | Correction of 3GPP IM CN subsystem XML handling                   | 8.3.0 | 8.4.0 | C1-081481 |
| 2008-06        | CP-40 | CP-080353 | 2221 | 1   | Media transcoding control functionality in IBCF                   | 8.3.0 | 8.4.0 | C1-081347 |
| 2008-06        | CP-40 | CP-080353 | 2219 | 1   | PANI header coding  | 8.3.0 | 8.4.0 | C1-081345 |
| 2008-06        | CP-40 | CP-080353 | 2209 | 1   | Alias URI   | 8.3.0 | 8.4.0 | C1-081343 |

| Change history |       |           |      |     |   |       |       |           |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2008-06        | CP-40 | CP-080353 | 2136 | 7   | 3GPP IM CN subsystem XML Schema version   | 8.3.0 | 8.4.0 | C1-081480 |
| 2008-06        | CP-40 | CP-080353 | 2255 | 3   | Annex K: ICE procedures for the P-CSCF  | 8.3.0 | 8.4.0 | C1-081470 |
| 2008-06        | CP-40 | CP-080354 | 2284 | 2   | SDP Enhancements to support resource allocation   | 8.3.0 | 8.4.0 | C1-082045 |
| 2008-06        | CP-40 | CP-080354 | 2218 | 2   | B2BUA AS influence of filter criteria evaluation  | 8.3.0 | 8.4.0 | C1-082033 |
| 2008-06        | CP-40 | CP-080354 | 2263 | 1   | Multiple contact addresses  | 8.3.0 | 8.4.0 | C1-082041 |
| 2008-06        | CP-40 | CP-080354 | 2280 | -   | Annex A : SIP Record-Route header table correction  | 8.3.0 | 8.4.0 | C1-081605 |
| 2008-06        | CP-40 | CP-080354 | 2206 | 2   | "rport" and "received" parameters at P-CSCF   | 8.3.0 | 8.4.0 | C1-081871 |
| 2008-06        | CP-40 | CP-080354 | 2282 | 1   | Display Name in Reg Event   | 8.3.0 | 8.4.0 | C1-082027 |
| 2008-06        | CP-40 | CP-080354 | 2285 | -   | Update IETF draft reference   | 8.3.0 | 8.4.0 | C1-081701 |
| 2008-06        | CP-40 | CP-080354 | 2207 | 2   | UE handling the "rport" parameter   | 8.3.0 | 8.4.0 | C1-081872 |
| 2008-06        | CP-40 | CP-080355 | 2234 | 4   | Annex K alignment with main body and cleanup  | 8.3.0 | 8.4.0 | C1-082043 |
| 2008-06        | CP-40 | CP-080355 | 2291 | 1   | Determining when to invoke SIP Digest procedures in S-CSCF  | 8.3.0 | 8.4.0 | C1-081944 |
| 2008-06        | CP-40 | CP-080355 | 2269 | 1   | Cleanup of SIP Digest/TLS procedures  | 8.3.0 | 8.4.0 | C1-081942 |
| 2008-06        | CP-40 | CP-080359 | 2260 | 2   | P-CSCF: Aligning P-Profile-Key behaviour for Wildcarded public user identities with Wildcarded PSI            | 8.3.0 | 8.4.0 | C1-081476 |
| 2008-06        | CP-40 | CP-080359 | 2212 | 4   | Dial string handling  | 8.3.0 | 8.4.0 | C1-082110 |
| 2008-06        | CP-40 | CP-080359 | 2261 | 2   | Trustdomain: Adding P-Profile-Key header to the trustdomain   | 8.3.0 | 8.4.0 | C1-081477 |
| 2008-06        | CP-40 | CP-080359 | 2239 | 1   | Trust domain changes for identity headers for business communication  | 8.3.0 | 8.4.0 | C1-081206 |
| 2008-06        | CP-40 | CP-080359 | 2259 | 2   | I-CSCF: Aligning P-Profile-Key behaviour for Wildcarded public user identities with Wildcarded PSI procedures | 8.3.0 | 8.4.0 | C1-081475 |
| 2008-06        | CP-40 | CP-080359 | 2232 | 2   | Delivering Request-URI to UE managing several terminals   | 8.3.0 | 8.4.0 | C1-081474 |
| 2008-06        | CP-40 | CP-080359 | 2262 | -   | Private network indication annex A changes  | 8.3.0 | 8.4.0 | C1-081210 |
| 2008-06        | CP-40 | CP-080359 | 2240 | 3   | Handling of private network indication  | 8.3.0 | 8.4.0 | C1-081953 |
| 2008-06        | CP-40 | CP-080360 | 2273 | 1   | Event package usage for Message Waiting Indication (MWI) service  | 8.3.0 | 8.4.0 | C1-081901 |
| 2008-06        | CP-40 | CP-080360 | 2226 | 3   | XML-support of transit specific content Tables  | 8.3.0 | 8.4.0 | C1-081905 |
| 2008-06        | CP-40 | CP-080364 | 2222 | 3   | Depth of IMS service level trace  | 8.3.0 | 8.4.0 | C1-081955 |
| 2008-06        | CP-40 | CP-080366 | 2252 | 1   | Emergency CS call set up procedures for non-3GPP systems  | 8.3.0 | 8.4.0 | C1-081465 |
| 2008-06        | CP-40 | CP-080366 | 2268 | 1   | Different IP addresses  | 8.3.0 | 8.4.0 | C1-081945 |
| 2008-06        | CP-40 | CP-080366 | 2251 | 1   | Remove specific codec requirement   | 8.3.0 | 8.4.0 | C1-081464 |
| 2008-06        | CP-40 | CP-080400 | 2208 | 2   | "rport" parameter   | 8.3.0 | 8.4.0 | -         |
| 2008-06        | CP-40 | CP-080402 | 2296 | -   | IARI and ICSI in different feature tags   | 8.3.0 | 8.4.0 | -         |
| 2008-06        | CP-40 | CP-080417 | 2211 | 5   | Call forwarding in IMS  | 8.3.0 | 8.4.0 | -         |
| 2008-06        |       |           |      |     | Editorial change done by MCC  | 8.4.0 | 8.4.1 |           |

| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2008-09        | CP-41 | CP-080643 | 2177 | 7   | Allow Multiple Registrations in Rel 8 by using Outbound                        | 8.4.1 | 8.5.0 |           |
| 2008-09        | CP-41 | CP-080539 | 2178 | 6   | Add Timestamp in Register Request  | 8.4.1 | 8.5.0 | C1-082810 |
| 2008-09        | CP-41 | CP-080527 | 2297 | 1   | Cleanup of P-CSCF procedures for inclusion of "tls-yes" and "tls-pending"      | 8.4.1 | 8.5.0 | C1-082623 |
| 2008-09        | CP-41 | CP-080538 | 2298 | 1   | Introduction of GIBA (Early IMS) procedures                                    | 8.4.1 | 8.5.0 | C1-082657 |
| 2008-09        | CP-41 | CP-080527 | 2299 | 1   | Add reference to draft-dotson-sip-mutual-auth                                  | 8.4.1 | 8.5.0 | C1-082621 |
| 2008-09        | CP-41 | CP-080523 | 2301 | 1   | Correction of DHCP reference   | 8.4.1 | 8.5.0 | C1-082620 |
| 2008-09        | CP-41 | CP-080523 | 2302 |     | Reference correction   | 8.4.1 | 8.5.0 | C1-082142 |
| 2008-09        | CP-41 | CP-080515 | 2306 | 1   | Annex A: Correction of SDP connection information                              | 8.4.1 | 8.5.0 | C1-082611 |
| 2008-09        | CP-41 | CP-080523 | 2308 | 1   | Backward compability issue with P-Access-Network-Info ABNF extension           | 8.4.1 | 8.5.0 | C1-082625 |
| 2008-09        | CP-41 | CP-080517 | 2314 |     | Addition of AVPF support and SDP capability negotiation mechanism              | 8.4.1 | 8.5.0 | C1-082268 |
| 2008-09        | CP-41 | CP-080520 | 2316 |     | Profile corrections for outbound   | 8.4.1 | 8.5.0 | C1-082270 |
| 2008-09        | CP-41 | CP-080531 | 2319 |     | Support of Direct Ethernet access as IP-CAN                                    | 8.4.1 | 8.5.0 | C1-082324 |
| 2008-09        | CP-41 | CP-080520 | 2323 | 1   | Update Outbound Reference  | 8.4.1 | 8.5.0 | C1-082626 |
| 2008-09        | CP-41 | CP-080523 | 2325 | 2   | Error Response for Different S-CSCF Assignment                                 | 8.4.1 | 8.5.0 | C1-082770 |
| 2008-09        | CP-41 | CP-080527 | 2328 | 1   | Annex K Technical Corrections  | 8.4.1 | 8.5.0 | C1-082622 |
| 2008-09        | CP-41 | CP-080528 | 2329 | 1   | Adding P-Debug-ID to SIP Profile Tables  | 8.4.1 | 8.5.0 | C1-082752 |
| 2008-09        | CP-41 | CP-080528 | 2330 | 2   | Subscribing to the debug event package   | 8.4.1 | 8.5.0 | C1-082781 |
| 2008-09        | CP-41 | CP-080522 | 2331 | 4   | EPS as IP-CAN  | 8.4.1 | 8.5.0 | C1-083637 |
| 2008-09        | CP-41 | CP-080523 | 2333 | 2   | Alignment of IP-CAN specific annexes   | 8.4.1 | 8.5.0 | C1-082778 |
| 2008-09        | CP-41 | CP-080516 | 2336 |     | Emergency PUID   | 8.4.1 | 8.5.0 | C1-082864 |
| 2008-09        | CP-41 | CP-080667 | 2340 | 3   | Initial emergency registration   | 8.4.1 | 8.5.0 |           |
| 2008-09        | CP-41 | CP-080516 | 2342 | 2   | Emergency session set-up   | 8.4.1 | 8.5.0 | C1-083532 |
| 2008-09        | CP-41 | CP-080516 | 2344 | 1   | P-CSCF handling of emergency sessions  | 8.4.1 | 8.5.0 | C1-083391 |
| 2008-09        | CP-41 | CP-080516 | 2346 | 3   | S-CSCF handling of emergency registration                                      | 8.4.1 | 8.5.0 | C1-083534 |
| 2008-09        | CP-41 | CP-080523 | 2347 | 1   | Informative Explanation and Corrections of Profile Tables                      | 8.4.1 | 8.5.0 | C1-083353 |
| 2008-09        | CP-41 | CP-080523 | 2350 | 1   | More than one contact address per UE   | 8.4.1 | 8.5.0 | C1-083351 |
| 2008-09        | CP-41 | CP-080528 | 2351 | 1   | IMS Trace for entities not on the path of the register request                 | 8.4.1 | 8.5.0 | C1-083383 |
| 2008-09        | CP-41 | CP-080528 | 2352 | 1   | Start and stop procedures for IMS trace  | 8.4.1 | 8.5.0 | C1-083384 |
| 2008-09        | CP-41 | CP-080636 | 2353 | 1   | Align emergency session handling outside a security association or TLS session | 8.4.1 | 8.5.0 |           |
| 2008-09        | CP-41 | CP-080637 | 2354 | 3   | Addressing privacy requirement   | 8.4.1 | 8.5.0 |           |
| 2008-09        | CP-41 | CP-080523 | 2359 | 2   | SDP Offer  | 8.4.1 | 8.5.0 | C1-083398 |
| 2008-09        | CP-41 | CP-080515 | 2362 |     | SDP referencing error for IBCF (IMS-ALG)                                       | 8.4.1 | 8.5.0 | C1-082927 |
| 2008-09        | CP-41 | CP-080523 | 2363 | 2   | Addition of draft-ietf-sip-199-00  | 8.4.1 | 8.5.0 | C1-083399 |



| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2008-09        | CP-41 | CP-080523 | 2365 | 1   | Usage of draft-holmberg-sip-keep-01 for emergency session                                    | 8.4.1 | 8.5.0 | C1-083395 |
| 2008-09        | CP-41 | CP-080537 | 2366 | 1   | Mediactrl and netann specifications  | 8.4.1 | 8.5.0 | C1-083363 |
| 2008-09        | CP-41 | CP-080536 | 2369 | 1   | S-CSCF and AS procedures with Enhanced Filter Criteria                                       | 8.4.1 | 8.5.0 | C1-083501 |
| 2008-09        | CP-41 | CP-080617 | 2371 | 2   | Correct handling for <reason> element  | 8.4.1 | 8.5.0 |           |
| 2008-09        | CP-41 | CP-080539 | 2375 |     | Modification of ci-3gpp2 parameter   | 8.4.1 | 8.5.0 | C1-083200 |
| 2008-09        | CP-41 | CP-080668 | 2377 | 3   | Alignment of usage of terms ISIM and ISIM Application  | 8.4.1 | 8.5.0 |           |
| 2008-09        | CP-41 | CP-080524 | 2378 | 1   | Introduction additional methods of P-CSCF discovery to support IMS Local Breakout            | 8.4.1 | 8.5.0 | C1-083400 |
| 2008-09        | CP-41 | CP-080515 | 2381 |     | Alignment with current version of draft-ietf-sip-fork-loop-fix                               | 8.4.1 | 8.5.0 | C1-083246 |
| 2008-09        | CP-41 | CP-080522 | 2386 | 1   | Relationship to IP-CAN   | 8.4.1 | 8.5.0 | C1-083424 |
| 2008-09        |       |           |      |     | Editorial change done by MCC   | 8.5.0 | 8.5.1 |           |
| 2008-12        | CP-42 | CP-080942 | 2324 | 9   | Introduction of IMC in support of common IMS   | 8.5.1 | 8.6.0 | -         |
| 2008-12        | CP-42 | CP-080847 | 2327 | 5   | SDP Enhancements to support resource allocation  | 8.5.1 | 8.6.0 | C1-084937 |
| 2008-12        | CP-42 | CP-080840 | 2332 | 3   | Additional changes for private network indication  | 8.5.1 | 8.6.0 | C1-084441 |
| 2008-12        | CP-42 | CP-080847 | 2358 | 7   | Prevent DDOS attack on PSAP  | 8.5.1 | 8.6.0 | C1-085454 |
| 2008-12        | CP-42 | CP-080840 | 2383 | 1   | Modifications to private network indication in profile                                       | 8.5.1 | 8.6.0 | C1-084080 |
| 2008-12        | CP-42 | CP-080847 | 2388 | 3   | Annex A fixes regarding draft-ietf-sip-199   | 8.5.1 | 8.6.0 | C1-085202 |
| 2008-12        | CP-42 | CP-080847 | 2389 | 1   | Annex A fixes regarding draft-holmberg-sip-keep  | 8.5.1 | 8.6.0 | C1-084278 |
| 2008-12        | CP-42 | CP-080847 | 2394 | -   | Correction on setting P-Served-User  | 8.5.1 | 8.6.0 | C1-083694 |
| 2008-12        | CP-42 | CP-080847 | 2396 | 1   | Clarification on ICSI and IARI   | 8.5.1 | 8.6.0 | C1-084203 |
| 2008-12        | CP-42 | CP-080847 | 2402 | 2   | Interface identifier   | 8.5.1 | 8.6.0 | C1-085204 |
| 2008-12        | CP-42 | CP-080844 | 2403 | 2   | UE subscription to reg-evet  | 8.5.1 | 8.6.0 | C1-084420 |
| 2008-12        | CP-42 | CP-080844 | 2405 | 3   | UE - multiple contacts registration  | 8.5.1 | 8.6.0 | C1-085205 |
| 2008-12        | CP-42 | CP-080844 | 2406 | 1   | UE - multiple contacts authentication and deregistration                                     | 8.5.1 | 8.6.0 | C1-084282 |
| 2008-12        | CP-42 | CP-080844 | 2407 | 1   | UE using multiple contacts   | 8.5.1 | 8.6.0 | C1-084283 |
| 2008-12        | CP-42 | CP-080845 | 2408 | 4   | Introduction of additional methods of P-CSCF discovery for EPS to support IMS Local Breakout | 8.5.1 | 8.6.0 | C1-085206 |
| 2008-12        | CP-42 | CP-080956 | 2409 | 5   | UE procedures when multiple P-CSCF discovery procedures are supported                        | 8.5.1 | 8.6.0 | -         |
| 2008-12        | CP-42 | CP-080854 | 2411 | 1   | Cr addition to section 4   | 8.5.1 | 8.6.0 | C1-084230 |
| 2008-12        | CP-42 | CP-080854 | 2412 | 2   | Netann, mediactrl text improvements  | 8.5.1 | 8.6.0 | C1-084434 |
| 2008-12        | CP-42 | CP-080854 | 2413 | 2   | Media control for charging, delegation   | 8.5.1 | 8.6.0 | C1-085256 |
| 2008-12        | CP-42 | CP-080847 | 2421 | -   | Trademark CDMA terminology   | 8.5.1 | 8.6.0 | C1-083983 |
| 2008-12        | CP-42 | CP-080843 | 2423 | 2   | Aligning initial INVITE request usage of Accept header field and profile tables              | 8.5.1 | 8.6.0 | C1-084438 |
| 2008-12        | CP-42 | CP-080858 | 2424 | 1   | Clarification of security-verify for TLS   | 8.5.1 | 8.6.0 | C1-084234 |

| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2008-12        | CP-42 | CP-080840 | 2425 | 2   | Setting of the Phone-context parameter when IP-CAN is Ethernet                         | 8.5.1 | 8.6.0 | C1-085201 |
| 2008-12        | CP-42 | CP-080847 | 2427 | -   | P-CSCF call release upon reception of indication that no resource is available.        | 8.5.1 | 8.6.0 | C1-084024 |
| 2008-12        | CP-42 | CP-080847 | 2428 | 2   | Removing of the cpc parameter by the terminating S-CSCF removes CPC                    | 8.5.1 | 8.6.0 | C1-084435 |
| 2008-12        | CP-42 | CP-080844 | 2430 | 2   | Clarification of abnormal case for deregistration                                      | 8.5.1 | 8.6.0 | C1-085158 |
| 2008-12        | CP-42 | CP-080847 | 2431 | -   | P-CSCF handling of "integrity-protected"   | 8.5.1 | 8.6.0 | C1-084048 |
| 2008-12        | CP-42 | CP-080839 | 2432 | 2   | Registration Procedure for ICS   | 8.5.1 | 8.6.0 | C1-085200 |
| 2008-12        | CP-42 | CP-080870 | 2434 | 1   | SMSIP related changes for the profile tables   | 8.5.1 | 8.6.0 | C1-084202 |
| 2008-12        | CP-42 | CP-080853 | 2435 | 1   | Adding roles defined for service level interworking for messaging to the profile table | 8.5.1 | 8.6.0 | C1-084270 |
| 2008-12        | CP-42 | CP-080840 | 2436 | -   | Downloading of information to the P-CSCF   | 8.5.1 | 8.6.0 | C1-084082 |
| 2008-12        | CP-42 | CP-080835 | 2440 | 2   | Adding reference to Internet Draft on sos URI parameter for emergency calls            | 8.5.1 | 8.6.0 | C1-085260 |
| 2008-12        | CP-42 | CP-080857 | 2441 | -   | Update reference for DAI Parameter for the "tel" URI                                   | 8.5.1 | 8.6.0 | C1-084120 |
| 2008-12        | CP-42 | CP-080847 | 2442 | 3   | Inclusion of draft-ietf-sip-body-handling in the profile tables                        | 8.5.1 | 8.6.0 | C1-085209 |
| 2008-12        | CP-42 | CP-080856 | 2443 | 3   | Deterministic Routing for overlap signalling   | 8.5.1 | 8.6.0 | C1-085239 |
| 2008-12        | CP-42 | CP-080840 | 2444 | 1   | Allowing P-Asserted Identity from an UE  | 8.5.1 | 8.6.0 | C1-085254 |
| 2008-12        | CP-42 | CP-080835 | 2446 | -   | Emergency call   | 8.5.1 | 8.6.0 | C1-084649 |
| 2008-12        | CP-42 | CP-080843 | 2448 | 1   | Deregistration in 200 (OK)   | 8.5.1 | 8.6.0 | C1-085435 |
| 2008-12        | CP-42 | CP-080939 | 2449 | 2   | Revision of 24.229-2449r1 (C1-085416)  | 8.5.1 | 8.6.0 | -         |
| 2008-12        | CP-42 | CP-080844 | 2450 | 2   | Usage of outbound in call setup  | 8.5.1 | 8.6.0 | C1-085450 |
| 2008-12        | CP-42 | CP-080844 | 2451 | -   | Multiple registrations at P-CSCF   | 8.5.1 | 8.6.0 | C1-084655 |
| 2008-12        | CP-42 | CP-080940 | 2452 | 2   | Revision of 24.229-2452r1 (C1-085418)  | 8.5.1 | 8.6.0 | -         |
| 2008-12        | CP-42 | CP-080844 | 2454 | 1   | Multiple registrations at S-CSCF   | 8.5.1 | 8.6.0 | C1-085419 |
| 2008-12        | CP-42 | CP-080869 | 2456 | -   | Correction of ICSI and IARI feature tag name   | 8.5.1 | 8.6.0 | C1-084689 |
| 2008-12        | CP-42 | CP-080862 | 2457 | 2   | Inclusion and Modification of Resource-Priority header at P-CSCF                       | 8.5.1 | 8.6.0 | C1-085451 |
| 2008-12        | CP-42 | CP-080854 | 2458 | 1   | Media control related profile table updates  | 8.5.1 | 8.6.0 | C1-085255 |
| 2008-12        | CP-42 | CP-080854 | 2459 | 1   | MediaCtrl reference updates  | 8.5.1 | 8.6.0 | C1-085257 |
| 2008-12        | CP-42 | CP-080839 | 2460 | 2   | Instance ID definition   | 8.5.1 | 8.6.0 | C1-085459 |
| 2008-12        | CP-42 | CP-080844 | 2462 | 2   | GRUU and Multiple registration   | 8.5.1 | 8.6.0 | C1-085468 |
| 2008-12        | CP-42 | CP-080959 | 2464 | 4   | Overlap signalling procedures  | 8.5.1 | 8.6.0 | -         |
| 2008-12        | CP-42 | CP-080841 | 2469 | -   | Reference updates (release 6 ietf dependencies)  | 8.5.1 | 8.6.0 | C1-084898 |
| 2008-12        | CP-42 | CP-080843 | 2471 | -   | Reference updates (release 7 ietf dependencies)  | 8.5.1 | 8.6.0 | C1-084903 |
| 2008-12        | CP-42 | CP-080858 | 2472 | 1   | No domain field for SIP digest   | 8.5.1 | 8.6.0 | C1-085261 |
| 2008-12        | CP-42 | CP-080858 | 2473 | 1   | Digest Authentication of Non-Register requests   | 8.5.1 | 8.6.0 | C1-085262 |

| Change history |       |           |      |     |   |       |       |           |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2008-12        | CP-42 | CP-080855 | 2477 | 1   | Minor corrections to configuration of entities for trace  | 8.5.1 | 8.6.0 | C1-085128 |
| 2008-12        | CP-42 | CP-080843 | 2479 | -   | Inclusion of missing RFC 3351 reference   | 8.5.1 | 8.6.0 | C1-085011 |
| 2008-12        | CP-42 | CP-080847 | 2480 | 2   | Documentation of INFO within the IM CN subsystem  | 8.5.1 | 8.6.0 | C1-085424 |
| 2008-12        | CP-42 | CP-080847 | 2481 | -   | Removal of TrGW normative requirements from IBCF  | 8.5.1 | 8.6.0 | C1-085015 |
| 2008-12        | CP-42 | CP-080847 | 2482 | -   | Editorial consistency and best practice   | 8.5.1 | 8.6.0 | C1-085016 |
| 2008-12        | CP-42 | CP-080965 | 2483 | 3   | Updates to profile tables to include ICS additions  | 8.5.1 | 8.6.0 | -         |
| 2008-12        | CP-42 | CP-080849 | 2484 | -   | Cleanup of various GIBA Editor's notes  | 8.5.1 | 8.6.0 | C1-085025 |
| 2008-12        | CP-42 | CP-080853 | 2485 | 1   | Addition of cpim/message and message/imdn+xml   | 8.5.1 | 8.6.0 | C1-085291 |
| 2008-12        | CP-42 | CP-080847 | 2494 | 3   | Documenting RFC 5373  | 8.5.1 | 8.6.0 | C1-085483 |
| 2008-12        | CP-42 | CP-080873 | 2495 | 1   | S-CSCF and AS procedures with Enhanced Filter Criteria  | 8.5.1 | 8.6.0 | C1-085292 |
| 2008-12        | CP-42 | CP-080847 | 2498 | 2   | Call release by the P-CSCF upon resource reservation failure  | 8.5.1 | 8.6.0 | C1-085467 |
| 2008-12        | CP-42 | CP-080847 | 2499 | 1   | Hosted NAT traversal for media flows  | 8.5.1 | 8.6.0 | C1-085430 |
| 2008-12        | CP-42 | CP-080846 | 2501 | 1   | Reference updates (release 8 ietf dependencies)   | 8.5.1 | 8.6.0 | C1-085426 |
| 2008-12        | CP-42 | CP-080847 | 2502 | -   | Corrections to security overview  | 8.5.1 | 8.6.0 | C1-085093 |
| 2008-12        | CP-42 | CP-080847 | 2505 | -   | Identification of public user identity in absence of Authorization header                           | 8.5.1 | 8.6.0 | C1-085131 |
| 2008-12        | CP-42 |           |      |     | Editorial cleanup by ETSI EditHelp! and MCC   | 8.5.1 | 8.6.0 |           |
| 2009-03        | CP-43 | CP-090134 | 2438 | 7   | Correction of non UE detectable emergency call procedures   | 8.6.0 | 8.7.0 | C1-091088 |
| 2009-03        | CP-43 | CP-090121 | 2507 |     | Correction of URN-value for Service Identifiers   | 8.6.0 | 8.7.0 | C1-090012 |
| 2009-03        | CP-43 | CP-090134 | 2508 | 1   | Re-selection of S-CSCF during Terminating and Originating Procedures                                | 8.6.0 | 8.7.0 | C1-090991 |
| 2009-03        | CP-43 | CP-090146 | 2509 | 2   | Re-selection of S-CSCF during Terminating and Originating Procedures when restoration is supported. | 8.6.0 | 8.7.0 | C1-091066 |
| 2009-03        | CP-43 | CP-090245 | 2510 | 4   | Returning an error to trigger a new registration when IMS restoration is supported                  | 8.6.0 | 8.7.0 | -         |
| 2009-03        | CP-43 | CP-090225 | 2511 | 4   | Re-selection of S-CSCF during Re-registration when IMS restoration is supported                     | 8.6.0 | 8.7.0 | -         |
| 2009-03        | CP-43 | CP-090134 | 2514 | 1   | Outbound with IMS AKA   | 8.6.0 | 8.7.0 | C1-090992 |
| 2009-03        | CP-43 | CP-090134 | 2515 | 2   | Registration procedure at the S-CSCF  | 8.6.0 | 8.7.0 | C1-091041 |
| 2009-03        | CP-43 | CP-090134 | 2516 | 3   | P-CSCFprocessing 200 (OK)   | 8.6.0 | 8.7.0 | C1-091085 |
| 2009-03        | CP-43 | CP-090134 | 2517 | 4   | Multiple de-registrations   | 8.6.0 | 8.7.0 | C1-091111 |
| 2009-03        | CP-43 | CP-090134 | 2519 | 1   | Instance-ID in INVITE   | 8.6.0 | 8.7.0 | C1-090997 |
| 2009-03        | CP-43 | CP-090134 | 2520 |     | Multiple contact addresses  | 8.6.0 | 8.7.0 | C1-090042 |
| 2009-03        | CP-43 | CP-090130 | 2524 | 3   | Support for eHRPD   | 8.6.0 | 8.7.0 | C1-091381 |
| 2009-03        | CP-43 | CP-090155 | 2525 | 1   | Adding the role of The Early Session Disposition Type   | 8.6.0 | 8.7.0 | C1-090950 |

| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2009-03        | CP-43 | CP-090134 | 2527 |     | Cleanup inclusion of draft-ietf-sip-body-handling in the profile tables                  | 8.6.0 | 8.7.0 | C1-090201 |
| 2009-03        | CP-43 | CP-090116 | 2529 | 2   | Aligning with draft-ietf-sip-location-conveyance-12                                      | 8.6.0 | 8.7.0 | C1-091040 |
| 2009-03        | CP-43 | CP-090134 | 2530 | 1   | Addressing privacy requirement for emergency calls                                       | 8.6.0 | 8.7.0 | C1-090999 |
| 2009-03        | CP-43 | CP-090116 | 2532 | 1   | Correcting condition for using indicating use of emergency registration                  | 8.6.0 | 8.7.0 | C1-090959 |
| 2009-03        | CP-43 | CP-090224 | 2534 | 3   | Overlap signalling en-bloc conversion procedures   | 8.6.0 | 8.7.0 | -         |
| 2009-03        | CP-43 | CP-090209 | 2535 | 3   | Overlap signalling digit collection procedures   | 8.6.0 | 8.7.0 | -         |
| 2009-03        | CP-43 | CP-090134 | 2537 | 1   | Correction of registration duration value  | 8.6.0 | 8.7.0 | C1-091024 |
| 2009-03        | CP-43 | CP-090127 | 2540 | 1   | Corrections to E-UTRAN specific aspects  | 8.6.0 | 8.7.0 | C1-090850 |
| 2009-03        | CP-43 | CP-090134 | 2541 |     | Miscellaneous corrections to annex B   | 8.6.0 | 8.7.0 | C1-090377 |
| 2009-03        | CP-43 | CP-090142 | 2543 | 1   | Miscellaneous corrections to Annex M   | 8.6.0 | 8.7.0 | C1-090985 |
| 2009-03        | CP-43 | CP-090142 | 2544 | 1   | Phone-context parameter value for cdma2000®  | 8.6.0 | 8.7.0 | C1-090986 |
| 2009-03        | CP-43 | CP-090142 | 2545 | 1   | Common IMS for MGW and MRF   | 8.6.0 | 8.7.0 | C1-090987 |
| 2009-03        | CP-43 | CP-090134 | 2546 | 4   | Deterministic behaviour for Call Forwarding  | 8.6.0 | 8.7.0 | C1-091122 |
| 2009-03        | CP-43 | CP-090136 | 2547 | 1   | Overlap Corrections  | 8.6.0 | 8.7.0 | C1-090962 |
| 2009-03        | CP-43 | CP-090116 | 2550 | 1   | Alignment of emergency indication with draft-patel-ecrit-sos-parameter-03                | 8.6.0 | 8.7.0 | C1-090968 |
| 2009-03        | CP-43 | CP-090272 | 2553 | 3   | Use of multiple access technologies in IMS   | 8.6.0 | 8.7.0 | -         |
| 2009-03        | CP-43 | CP-090134 | 2555 |     | Alignment of authentication parameter terminology  | 8.6.0 | 8.7.0 | C1-090534 |
| 2009-03        | CP-43 | CP-090134 | 2556 |     | Use of access-class and access-type constructs in the P-Access-Network-Info header field | 8.6.0 | 8.7.0 | C1-090535 |
| 2009-03        | CP-43 | CP-090134 | 2558 |     | P-Served-User header field corrections (profile)   | 8.6.0 | 8.7.0 | C1-090537 |
| 2009-03        | CP-43 | CP-090134 | 2560 |     | Editorial consistency and best practice  | 8.6.0 | 8.7.0 | C1-090539 |
| 2009-03        | CP-43 | CP-090141 | 2561 | 1   | Removal of redundant NASS bundled authentication text for S-CSCF                         | 8.6.0 | 8.7.0 | C1-090969 |
| 2009-03        | CP-43 | CP-090150 | 2564 | 1   | Emergency call handling for CS media   | 8.6.0 | 8.7.0 | C1-090908 |
| 2009-03        | CP-43 | CP-090118 | 2574 | 2   | Correction to Annex A / SIP extensions for media authorization                           | 8.6.0 | 8.7.0 | C1-091120 |
| 2009-03        | CP-43 | CP-090275 | 2578 | 4   | Correction to Annex A /P-Access-Network-Info   | 8.6.0 | 8.7.0 | -         |
| 2009-03        | CP-43 | CP-090134 | 2579 | 2   | Correction to Annex A /P-User-Database header  | 8.6.0 | 8.7.0 | C1-091084 |
| 2009-03        | CP-43 | CP-090134 | 2582 | 2   | Routeing B2BUA transparency  | 8.6.0 | 8.7.0 | C1-091078 |
| 2009-03        | CP-43 | CP-090134 | 2583 | 1   | Call release by P-CSCF- Editorial correction   | 8.6.0 | 8.7.0 | C1-091013 |
| 2009-03        | CP-43 | CP-090118 | 2584 | 1   | References correction  | 8.6.0 | 8.7.0 | C1-091014 |
| 2009-03        | CP-43 | CP-090142 | 2595 | 1   | Corrections for cdma2000® HRPD Emergency Services  | 8.6.0 | 8.7.0 | C1-090988 |
| 2009-03        | CP-43 | CP-090127 | 2596 |     | Corrections to EPS as IMS access technology Annex  | 8.6.0 | 8.7.0 | C1-090685 |
| 2009-03        | CP-43 | CP-090135 | 2597 | 1   | Update of references to SIP debug internet drafts  | 8.6.0 | 8.7.0 | C1-090970 |
| 2009-03        | CP-43 | CP-090159 | 2598 | 1   | Handling of provisioned mode of the resource allocation used for IMS media               | 8.6.0 | 8.7.0 | C1-091069 |

| Change history |       |           |      |     |   |       |       |           |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2009-03        | CP-43 | CP-090237 | 2601 | 2   | Reference correction  | 8.6.0 | 8.7.0 | C1-091115 |
| 2009-06        | CP-44 | CP-090428 | 2518 | 5   | Flow- token in the Record-Route   | 8.7.0 | 8.8.0 | C1-091475 |
| 2009-06        | CP-44 | CP-090398 | 2539 | 8   | Mechanism for UE to identify a SIP URI that has an associated tel URI                               | 8.7.0 | 8.8.0 | C1-092241 |
| 2009-06        | CP-44 | CP-090428 | 2557 | 3   | Application server usage of P-Served-User header field  | 8.7.0 | 8.8.0 | C1-092077 |
| 2009-06        | CP-44 | CP-090399 | 2605 | 2   | P-CSCF releasing a dialog   | 8.7.0 | 8.8.0 | C1-092084 |
| 2009-06        | CP-44 | CP-090399 | 2607 | 2   | S-CSCF releasing a dialog   | 8.7.0 | 8.8.0 | C1-092086 |
| 2009-06        | CP-44 | CP-090428 | 2608 | 2   | GRUU translation  | 8.7.0 | 8.8.0 | C1-092087 |
| 2009-06        | CP-44 | CP-090428 | 2610 | 1   | Correct backwards emergency notification procedure  | 8.7.0 | 8.8.0 | C1-092072 |
| 2009-06        | CP-44 | CP-090428 | 2611 |     | Correction of implementation error of CR2537r1  | 8.7.0 | 8.8.0 | C1-091494 |
| 2009-06        | CP-44 | CP-090428 | 2612 | 1   | BGCF routing  | 8.7.0 | 8.8.0 | C1-092074 |
| 2009-06        | CP-44 | CP-090403 | 2614 |     | Correction of 3GPP URN link   | 8.7.0 | 8.8.0 | C1-091504 |
| 2009-06        | CP-44 | CP-090428 | 2616 | 2   | RFC 2833 substituted by RFC 4733  | 8.7.0 | 8.8.0 | C1-092050 |
| 2009-06        | CP-44 | CP-090428 | 2617 |     | Call Forwarding Leftover  | 8.7.0 | 8.8.0 | C1-091510 |
| 2009-06        | CP-44 | CP-090415 | 2618 | 1   | Correction Identity handling for NGCN   | 8.7.0 | 8.8.0 | C1-091974 |
| 2009-06        | CP-44 | CP-090419 | 2619 |     | Reference Update draft-ietf-mmusic-sdp-cs   | 8.7.0 | 8.8.0 | C1-091513 |
| 2009-06        | CP-44 | CP-090428 | 2620 | 1   | RFC reference fix   | 8.7.0 | 8.8.0 | C1-092075 |
| 2009-06        | CP-44 | CP-090428 | 2625 | 1   | Deterministic XML schema  | 8.7.0 | 8.8.0 | C1-092204 |
| 2009-06        | CP-44 | CP-090398 | 2634 |     | Emergency call treatment of P-Preferred-Identity header field in profile                            | 8.7.0 | 8.8.0 | C1-091649 |
| 2009-06        | CP-44 | CP-090405 | 2635 | 1   | Subdivision of digit collection text  | 8.7.0 | 8.8.0 | C1-091967 |
| 2009-06        | CP-44 | CP-090428 | 2636 |     | Editorial changes   | 8.7.0 | 8.8.0 | C1-091655 |
| 2009-06        | CP-44 | CP-090398 | 2639 | 1   | Correcting emergency registration support and access type   | 8.7.0 | 8.8.0 | C1-092003 |
| 2009-06        | CP-44 | CP-090397 | 2645 | 1   | Correction to Annex A /Caller preferences directives  | 8.7.0 | 8.8.0 | C1-092079 |
| 2009-06        | CP-44 | CP-090428 | 2657 | 2   | Alignment of Cx reference point procedures with TS 29.228 procedures                                | 8.7.0 | 8.8.0 | C1-092211 |
| 2009-06        | CP-44 | CP-090415 | 2658 | 2   | Correction to GRUU procedures to ensure that sessions using UE assigned Public GRUUs don't fail     | 8.7.0 | 8.8.0 | C1-092219 |
| 2009-06        | CP-44 | CP-090428 | 2659 |     | Removing obsolete Editor's Note   | 8.7.0 | 8.8.0 | C1-091854 |
| 2009-06        | CP-44 | CP-090428 | 2660 | 1   | Correction of instance ID related Editor's Note and text  | 8.7.0 | 8.8.0 | C1-092076 |
| 2009-06        | CP-44 | CP-090398 | 2662 |     | Version update for "sos" URI parameter Internet Draft   | 8.7.0 | 8.8.0 | C1-091857 |
| 2009-06        | CP-44 | CP-090428 | 2663 |     | Contact Header in PUBLISH method  | 8.7.0 | 8.8.0 | C1-091879 |
| 2009-06        | CP-44 | CP-090428 | 2666 |     | Removing non-essential and incorrect statement regarding ordering of codec formats in the SDP offer | 8.7.0 | 8.8.0 | C1-092114 |
| 2009-06        | CP-44 | CP-090400 | 2667 | 1   | Correction to Annex A /P-User-Database  | 8.7.0 | 8.8.0 | C1-092209 |

| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2009-06        | CP-44 | CP-090430 | 2644 | 2   | Addition of capability for delivering the original Request-URI                     | 8.8.0 | 9.0.0 | C1-092227 |
| 2009-09        | CP-45 | CP-090696 | 2671 | 2   | Service-Route/Path header handling for fetching bindings                           | 9.0.0 | 9.1.0 | C1-093049 |
| 2009-09        | CP-45 | CP-090644 | 2674 | 2   | Inconsistency between text and XML schema  | 9.0.0 | 9.1.0 | C1-093709 |
| 2009-09        | CP-45 | CP-090650 | 2675 |     | Confusing text in L.2.2.5.1A   | 9.0.0 | 9.1.0 | C1-092401 |
| 2009-09        | CP-45 | CP-090658 | 2676 | 3   | Emergency call handling in P-CSCF and UE   | 9.0.0 | 9.1.0 | C1-093070 |
| 2009-09        | CP-45 | CP-090649 | 2679 | 1   | TISPAN IBCF review comment fixes   | 9.0.0 | 9.1.0 | C1-092903 |
| 2009-09        | CP-45 | CP-090696 | 2680 |     | TISPAN review comments - minor fixes   | 9.0.0 | 9.1.0 | C1-092407 |
| 2009-09        | CP-45 | CP-090657 | 2682 | 1   | Contact port in non REGISTER request with AKA                                      | 9.0.0 | 9.1.0 | C1-092409 |
| 2009-09        | CP-45 | CP-090696 | 2684 | 1   | reg/debug event package subscription headers                                       | 9.0.0 | 9.1.0 | C1-092987 |
| 2009-09        | CP-45 | CP-090664 | 2686 | 2   | Connection of complex UEs to IMS   | 9.0.0 | 9.1.0 | C1-093739 |
| 2009-09        | CP-45 | CP-090737 | 2689 | 2   | Calling party category (cpc)   | 9.0.0 | 9.1.0 | -         |
| 2009-09        | CP-45 | CP-090696 | 2691 | 1   | UE procedure on registration failure   | 9.0.0 | 9.1.0 | C1-093015 |
| 2009-09        | CP-45 | CP-090658 | 2693 | 1   | Correction of BGCF procedures  | 9.0.0 | 9.1.0 | C1-092989 |
| 2009-09        | CP-45 | CP-090696 | 2694 | 2   | Topology hiding on Path header   | 9.0.0 | 9.1.0 | C1-093016 |
| 2009-09        | CP-45 | CP-090682 | 2695 | 1   | Create XML source files  | 9.0.0 | 9.1.0 | C1-093029 |
| 2009-09        | CP-45 | CP-090667 | 2697 | 1   | Correcting preventing of DDOS attack on registrar                                  | 9.0.0 | 9.1.0 | C1-092952 |
| 2009-09        | CP-45 | CP-090657 | 2700 |     | Correcting mismatch in conditions for non-UE detectable emergency call             | 9.0.0 | 9.1.0 | C1-092494 |
| 2009-09        | CP-45 | CP-090659 | 2702 | 1   | The "comp" parameter   | 9.0.0 | 9.1.0 | C1-093702 |
| 2009-09        | CP-45 | CP-090659 | 2704 |     | Routing procedure  | 9.0.0 | 9.1.0 | C1-092501 |
| 2009-09        | CP-45 | CP-090664 | 2706 |     | UE as an externally attached network   | 9.0.0 | 9.1.0 | C1-092503 |
| 2009-09        | CP-45 | CP-090725 | 2710 | 2   | Require with the option-tag "outbound"   | 9.0.0 | 9.1.0 | -         |
| 2009-09        | CP-45 | CP-090658 | 2712 | 1   | Outbound support   | 9.0.0 | 9.1.0 | C1-092994 |
| 2009-09        | CP-45 | CP-090657 | 2718 | 2   | Contact header in registration   | 9.0.0 | 9.1.0 | C1-093704 |
| 2009-09        | CP-45 | CP-090659 | 2720 | 1   | S-CSCF not supporting Outbound registration  | 9.0.0 | 9.1.0 | C1-093002 |
| 2009-09        | CP-45 | CP-090648 | 2722 | 2   | NAT traversal without outbound   | 9.0.0 | 9.1.0 | C1-093041 |
| 2009-09        | CP-45 | CP-090651 | 2724 |     | Duplicate subclauses in Annex O  | 9.0.0 | 9.1.0 | C1-092530 |
| 2009-09        | CP-45 | CP-090664 | 2727 | 2   | P-CSCF handling alignments for privileged senders                                  | 9.0.0 | 9.1.0 | C1-093486 |
| 2009-09        | CP-45 | CP-090664 | 2729 | 1   | P-CSCF handling for NCGN as regular UE   | 9.0.0 | 9.1.0 | C1-092932 |
| 2009-09        | CP-45 | CP-090664 | 2731 | 5   | S-CSCF handling alignments for NGCN  | 9.0.0 | 9.1.0 | C1-093910 |
| 2009-09        | CP-45 | CP-090664 | 2741 | 2   | Use of GRUU by UEs that perform the functions of an external attached network      | 9.0.0 | 9.1.0 | C1-093905 |
| 2009-09        | CP-45 | CP-090658 | 2743 |     | Correction of alignment of Cx reference point procedures with TS 29.228 procedures | 9.0.0 | 9.1.0 | C1-092658 |
| 2009-09        | CP-45 | CP-090659 | 2745 |     | Reference update for draft-montemurro-gsma-imei-urn                                | 9.0.0 | 9.1.0 | C1-092660 |
| 2009-09        | CP-45 | CP-090696 | 2746 | 1   | Annex K: P-CSCF alignment  | 9.0.0 | 9.1.0 | C1-093017 |

| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2009-09        | CP-45 | CP-090696 | 2747 | 1   | Annex K: S-CSCF alignment  | 9.0.0 | 9.1.0 | C1-093018 |
| 2009-09        | CP-45 | CP-090696 | 2748 |     | Annex K: Removal of IBCF modifications   | 9.0.0 | 9.1.0 | C1-092664 |
| 2009-09        | CP-45 | CP-090658 | 2752 | 2   | Keep-alives for emergency calls  | 9.0.0 | 9.1.0 | C1-093043 |
| 2009-09        | CP-45 | CP-090649 | 2755 | 1   | P-CSCF forwarding request towards entry point  | 9.0.0 | 9.1.0 | C1-092910 |
| 2009-09        | CP-45 | CP-090659 | 2759 | 1   | Re-INVITE for precondition status indication   | 9.0.0 | 9.1.0 | C1-093011 |
| 2009-09        | CP-45 | CP-090658 | 2761 | 1   | Digest URI verification fix  | 9.0.0 | 9.1.0 | C1-093034 |
| 2009-09        | CP-45 | CP-090696 | 2762 |     | SDP in session modification messages   | 9.0.0 | 9.1.0 | C1-092678 |
| 2009-09        | CP-45 | CP-090658 | 2764 |     | Correction of table condition: AoC roles   | 9.0.0 | 9.1.0 | C1-092680 |
| 2009-09        | CP-45 | CP-090732 | 2766 | 5   | Aligning IANA registration of MIME type "application/3gpp-ims+xml"                       | 9.0.0 | 9.1.0 | -         |
| 2009-09        | CP-45 | CP-090690 | 2767 | 4   | Emergency call introduction  | 9.0.0 | 9.1.0 | C1-093946 |
| 2009-09        | CP-45 | CP-090690 | 2768 | 1   | Emergency call changes to Annex B (GPRS)   | 9.0.0 | 9.1.0 | C1-092825 |
| 2009-09        | CP-45 | CP-090690 | 2769 | 1   | Emergency call changes to Annex L (EPS)  | 9.0.0 | 9.1.0 | C1-092826 |
| 2009-09        | CP-45 | CP-090667 | 2778 | 1   | How the P-CSCF forwards the request to the next hop excluding the REGISTER method.       | 9.0.0 | 9.1.0 | C1-093006 |
| 2009-09        | CP-45 | CP-090696 | 2779 | 1   | Clarification of a target refresh request.   | 9.0.0 | 9.1.0 | C1-093007 |
| 2009-09        | CP-45 | CP-090660 | 2780 | 1   | No Proxy-Authentication-Info header  | 9.0.0 | 9.1.0 | C1-093721 |
| 2009-09        | CP-45 | CP-090664 | 2781 | 2   | No P-P-I from NGCN   | 9.0.0 | 9.1.0 | C1-093790 |
| 2009-09        | CP-45 | CP-090696 | 2784 | 1   | Trust domain clarification   | 9.0.0 | 9.1.0 | C1-093753 |
| 2009-09        | CP-45 | CP-090696 | 2785 | 1   | Clarification of Handling of geo-local numbers   | 9.0.0 | 9.1.0 | C1-093754 |
| 2009-09        | CP-45 | CP-090645 | 2789 |     | IOI Handling   | 9.0.0 | 9.1.0 | C1-093266 |
| 2009-09        | CP-45 | CP-090671 | 2791 | 1   | Invalid Registration   | 9.0.0 | 9.1.0 | C1-093745 |
| 2009-09        | CP-45 | CP-090665 | 2793 | 1   | IBCF and P-Asserted-Identity   | 9.0.0 | 9.1.0 | C1-093783 |
| 2009-09        | CP-45 | CP-090657 | 2797 | 1   | Correct the preconditions for NBA mechanism  | 9.0.0 | 9.1.0 | C1-093760 |
| 2009-09        | CP-45 | CP-090682 | 2800 | 4   | Correction of dialog correlation   | 9.0.0 | 9.1.0 | C1-093985 |
| 2009-09        | CP-45 | CP-090696 | 2801 |     | Corrections to SDP profile table entries   | 9.0.0 | 9.1.0 | C1-093449 |
| 2009-09        | CP-45 | CP-090657 | 2803 | 1   | Adding RFC 3890 and maximum packet rate to SDP profile tables                            | 9.0.0 | 9.1.0 | C1-093762 |
| 2009-09        | CP-45 | CP-090679 | 2806 | 2   | Correcting duplicate mentioning of 802.3y  | 9.0.0 | 9.1.0 | C1-093913 |
| 2009-09        | CP-45 | CP-090647 | 2813 |     | Update of reference to I-D for sos URI parameter and miscellaneous reference corrections | 9.0.0 | 9.1.0 | C1-093574 |
| 2009-09        | CP-45 | CP-090659 | 2815 | 2   | Use of ports for SIP between UE and P-CSCF   | 9.0.0 | 9.1.0 | C1-093908 |
| 2009-09        | CP-45 | CP-090659 | 2817 | 1   | Profile table correction on the support of security mechanism                            | 9.0.0 | 9.1.0 | C1-093578 |
| 2009-09        | CP-45 | CP-090696 | 2819 | 1   | Correction on the summary of security mechanism  | 9.0.0 | 9.1.0 | C1-093767 |
| 2009-09        | CP-45 | CP-090657 | 2827 | 1   | Clarification on identity usage for NBA  | 9.0.0 | 9.1.0 | C1-093769 |
| 2009-09        | CP-45 | CP-090664 | 2829 |     | Describe the right behaviour of the IBCF   | 9.0.0 | 9.1.0 | C1-093609 |
| 2009-12        | CP-46 | CP-090923 | 2834 | 3   | Correction to introduce support for IMSVoPS  | 9.1.0 | 9.2.0 | C1-095602 |
| 2009-12        | CP-46 | CP-090923 | 2835 | 2   | Transcoding Control at MRF using RFC 4117  | 9.1.0 | 9.2.0 | C1-094737 |

| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2009-12        | CP-46 | CP-090890 | 2839 |     | Inclusion of draft-ietf-sipcore-invfix   | 9.1.0 | 9.2.0 | C1-094120 |
| 2009-12        | CP-46 | CP-090890 | 2843 | 1   | Inclusion of draft-ietf-sip-ipv6-abnf-fix  | 9.1.0 | 9.2.0 | C1-094531 |
| 2009-12        | CP-46 | CP-090891 | 2847 |     | Change of ua-profile package to xcap-diff package  | 9.1.0 | 9.2.0 | C1-094131 |
| 2009-12        | CP-46 | CP-090892 | 2850 |     | Release 7 IETF reference updates for emergency call  | 9.1.0 | 9.2.0 | C1-094134 |
| 2009-12        | CP-46 | CP-090940 | 2854 |     | Inclusion of draft-ietf-sip-record-route-fix   | 9.1.0 | 9.2.0 | C1-094152 |
| 2009-12        | CP-46 | CP-090940 | 2855 | 1   | Correction of support of trust domain boundaries for identity                                    | 9.1.0 | 9.2.0 | C1-094566 |
| 2009-12        | CP-46 | CP-090923 | 2856 | 1   | Inclusion of roles for XCAP client / server at the Ut reference point for supplementary services | 9.1.0 | 9.2.0 | C1-094538 |
| 2009-12        | CP-46 | CP-090920 | 2858 |     | Update of draft-ietf-sip-body-handling reference to RFC 5621                                     | 9.1.0 | 9.2.0 | C1-094215 |
| 2009-12        | CP-46 | CP-090940 | 2860 |     | xsd file alignment with main document  | 9.1.0 | 9.2.0 | C1-094316 |
| 2009-12        | CP-46 | CP-090940 | 2861 | 1   | Textual layout errors in Annex A   | 9.1.0 | 9.2.0 | C1-094568 |
| 2009-12        | CP-46 | CP-090936 | 2863 | 2   | Media plane security   | 9.1.0 | 9.2.0 | C1-094729 |
| 2009-12        | CP-46 | CP-090940 | 2866 | 1   | 3rd party registration failure   | 9.1.0 | 9.2.0 | C1-094336 |
| 2009-12        | CP-46 | CP-090923 | 2689 | 4   | Detecting requests destined for a PSAP   | 9.1.0 | 9.2.0 | C1-095704 |
| 2009-12        | CP-46 | CP-091016 | 2875 | 5   | Alignment of 24.229 with draft-ietf-sipcore-info-events  | 9.1.0 | 9.2.0 | -         |
| 2009-12        | CP-46 | CP-090940 | 2877 | 1   | Correction of indication to the user that an emergency call was made                             | 9.1.0 | 9.2.0 | C1-094582 |
| 2009-12        | CP-46 | CP-090940 | 2881 | 2   | Annex A /183 (Session Progress) response   | 9.1.0 | 9.2.0 | C1-094733 |
| 2009-12        | CP-46 | CP-090890 | 2885 |     | Annex A / c and m paramters in media description in SDP  | 9.1.0 | 9.2.0 | C1-094382 |
| 2009-12        | CP-46 | CP-090890 | 2889 |     | Annex A / User-Agent in PUBLISH responses  | 9.1.0 | 9.2.0 | C1-094387 |
| 2009-12        | CP-46 | CP-091049 | 2891 | 3   | Annex A / Allow events   | 9.1.0 | 9.2.0 | -         |
| 2009-12        | CP-46 | CP-090940 | 2892 | 1   | Annex A /MIME-Version header   | 9.1.0 | 9.2.0 | C1-094571 |
| 2009-12        | CP-46 | CP-090940 | 2893 | 2   | Annex A / Require header   | 9.1.0 | 9.2.0 | C1-094734 |
| 2009-12        | CP-46 | CP-090940 | 2894 | 1   | Application of trust domains to the P-Early-media header field                                   | 9.1.0 | 9.2.0 | C1-094573 |
| 2009-12        | CP-46 | CP-090923 | 2895 | 2   | Allowing direct routing between AS and MRFC  | 9.1.0 | 9.2.0 | C1-094736 |
| 2009-12        | CP-46 | CP-090936 | 2900 | 3   | Registration of IMS media plane security capabilities  | 9.1.0 | 9.2.0 | C1-094730 |
| 2009-12        | CP-46 | CP-090893 | 2905 |     | Updating of outbound and related references  | 9.1.0 | 9.2.0 | C1-094826 |
| 2009-12        | CP-46 | CP-090894 | 2908 |     | Updating of GRUU references  | 9.1.0 | 9.2.0 | C1-094832 |
| 2009-12        | CP-46 | CP-090940 | 2909 |     | Miscellaneous editorial corrections  | 9.1.0 | 9.2.0 | C1-094850 |
| 2009-12        | CP-46 | CP-090892 | 2912 | 1   | Removal of outstanding Editor's notes for EMC1   | 9.1.0 | 9.2.0 | C1-095486 |
| 2009-12        | CP-46 | CP-090896 | 2914 |     | Removal of outstanding Editor's note for ServID  | 9.1.0 | 9.2.0 | C1-094855 |
| 2009-12        | CP-46 | CP-090903 | 2916 |     | Removal of outstanding Editor's note for Overlap   | 9.1.0 | 9.2.0 | C1-094857 |
| 2009-12        | CP-46 | CP-090940 | 2924 | 2   | Definition of globally Globally Routeable SIP URI.   | 9.1.0 | 9.2.0 | C1-095676 |



| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2009-12        | CP-46 | CP-090940 | 2925 | 1   | Handling of Request-URI with tel URI and sip URI containing user=phone by the BGCF   | 9.1.0 | 9.2.0 | C1-095438 |
| 2009-12        | CP-46 | CP-090940 | 2926 | 2   | Additional routeing capabilities   | 9.1.0 | 9.2.0 | C1-095677 |
| 2009-12        | CP-46 | CP-090902 | 2932 | 1   | Handling of Route by the I-CSCF  | 9.1.0 | 9.2.0 | C1-095607 |
| 2009-12        | CP-46 | CP-090902 | 2934 | 1   | Annex A/ P-Charging-Vector   | 9.1.0 | 9.2.0 | C1-095606 |
| 2009-12        | CP-46 | CP-090902 | 2936 | 2   | REGISTERS for Keeping NAT binding /Annex F   | 9.1.0 | 9.2.0 | C1-095703 |
| 2009-12        | CP-46 | CP-090938 | 2940 | 1   | MI reference point additions – general aspects                                       | 9.1.0 | 9.2.0 | C1-095467 |
| 2009-12        | CP-46 | CP-090938 | 2941 | 1   | MI reference point additions – location determination summary                        | 9.1.0 | 9.2.0 | C1-095468 |
| 2009-12        | CP-46 | CP-090938 | 2942 | 3   | MI reference point additions – E-CSCF changes  | 9.1.0 | 9.2.0 | C1-095726 |
| 2009-12        | CP-46 | CP-090938 | 2943 | 3   | MI reference point additions – new LRF functionality                                 | 9.1.0 | 9.2.0 | C1-095727 |
| 2009-12        | CP-46 | CP-090938 | 2944 |     | MI reference point additions – profile changes                                       | 9.1.0 | 9.2.0 | C1-094995 |
| 2009-12        | CP-46 | CP-090902 | 2946 |     | Correction of profile table on the role for UE                                       | 9.1.0 | 9.2.0 | C1-094997 |
| 2009-12        | CP-46 | CP-090936 | 2951 | 2   | Indicating End-to-Access Edge Media Plane Security in session set-up                 | 9.1.0 | 9.2.0 | C1-095700 |
| 2009-12        | CP-46 | CP-090895 | 2954 | 2   | Correct Phone-Context parameter coding   | 9.1.0 | 9.2.0 | C1-095688 |
| 2009-12        | CP-46 | CP-090940 | 2955 | 2   | Human readable UE name   | 9.1.0 | 9.2.0 | C1-095648 |
| 2009-12        | CP-46 | CP-090927 | 2959 | 2   | E-CSCF invoking EATF   | 9.1.0 | 9.2.0 | C1-095718 |
| 2009-12        | CP-46 | CP-090930 | 2960 | 2   | IMEI in unauthenticated emergency call in EPS and GPRS                               | 9.1.0 | 9.2.0 | C1-095714 |
| 2009-12        | CP-46 | CP-090930 | 2961 | 1   | Emergency bearer activation in EPS and GPRS  | 9.1.0 | 9.2.0 | C1-095309 |
| 2009-12        | CP-46 | CP-090892 | 2964 |     | Alignment of 24.229 with draft-patel-ecrit-sos-parameter-07                          | 9.1.0 | 9.2.0 | C1-095069 |
| 2009-12        | CP-46 | CP-090892 | 2967 | 1   | Removal of editor's note in 5.4.8.2 – use of "sos" in GRUU                           | 9.1.0 | 9.2.0 | C1-095489 |
| 2009-12        | CP-46 | CP-090923 | 2971 | 1   | Reason header in provisional responses   | 9.1.0 | 9.2.0 | C1-095472 |
| 2009-12        | CP-46 | CP-090940 | 2976 |     | Correcting SIP interface to VoiceXML media services                                  | 9.1.0 | 9.2.0 | C1-095187 |
| 2009-12        | CP-46 | CP-090940 | 2980 | 1   | Annex A: Support of INFO for CAT and CRS   | 9.1.0 | 9.2.0 | C1-095445 |
| 2009-12        | CP-46 | CP-090940 | 2981 | 2   | Removal of editor's note on 199 provisional response                                 | 9.1.0 | 9.2.0 | C1-095649 |
| 2009-12        | CP-46 | CP-090983 | 2970 | 2   | Update to annex J based on draft-patel-dispatch-cpc-oli-parameter                    | 9.1.0 | 9.2.0 | -         |
| 2010-03        | CP-47 | CP-100131 | 2810 | 3   | Correcting handling of emergency session requests made by unregistered users         | 9.2.0 | 9.3.0 | C1-101129 |
| 2010-03        | CP-47 | CP-100110 | 2930 | 4   | Handling of Request-URI with tel URI and sip URI containing user=phone by the S-CSCF | 9.2.0 | 9.3.0 | C1-100993 |
| 2010-03        | CP-47 | CP-100104 | 2958 | 4   | Emergency session with P-CSCF in visited network                                     | 9.2.0 | 9.3.0 | C1-100720 |
| 2010-03        | CP-47 | CP-100110 | 2990 | 1   | IETF reference updates (IMSProtoc2 related)  | 9.2.0 | 9.3.0 | C1-100210 |
| 2010-03        | CP-47 | CP-100124 | 2992 | 3   | Support of draft-ietf-mmusic-sdp-media-capabilities                                  | 9.2.0 | 9.3.0 | C1-101151 |
| 2010-03        | CP-47 | CP-100153 | 2994 | 5   | Adding 1XRTT Femto support for the 3GPP2-1X access type                              | 9.2.0 | 9.3.0 | C1-101180 |

| Change history |       |           |      |     |   |       |       |           |
|----------------|-------|-----------|------|-----|---|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old   | New   | WG doc    |
| 2010-03        | CP-47 | CP-100149 | 2996 | 1   | Correction for e2ae syntax  | 9.2.0 | 9.3.0 | C1-100200 |
| 2010-03        | CP-47 | CP-100153 | 2997 | 2   | Implications of resource reservation failure  | 9.2.0 | 9.3.0 | C1-100704 |
| 2010-03        | CP-47 | CP-100143 | 2998 | 1   | RFC 4488 in Annex A   | 9.2.0 | 9.3.0 | C1-100176 |
| 2010-03        | CP-47 | CP-100153 | 3000 | 1   | Removing an Editor's note in the reference section  | 9.2.0 | 9.3.0 | C1-100135 |
| 2010-03        | CP-47 | CP-100153 | 3001 | 4   | Handling of Subscription context information by intermediary entities   | 9.2.0 | 9.3.0 | C1-101116 |
| 2010-03        | CP-47 | CP-100151 | 3002 | 1   | Editorial update: adding missing defenitions, correcting typos and inconsistencies                                  | 9.2.0 | 9.3.0 | C1-100198 |
| 2010-03        | CP-47 | CP-100151 | 3003 | 3   | Correcting providing of additional location information to LRF  | 9.2.0 | 9.3.0 | C1-101117 |
| 2010-03        | CP-47 | CP-100149 | 3004 | 1   | Editorial amendments for end to access edge media security  | 9.2.0 | 9.3.0 | C1-100233 |
| 2010-03        | CP-47 | CP-100149 | 3005 | 2   | Improvements to end to access edge security text  | 9.2.0 | 9.3.0 | C1-100780 |
| 2010-03        | CP-47 | CP-100149 | 3006 | 1   | MGCF is not involved in e2ae security   | 9.2.0 | 9.3.0 | C1-100234 |
| 2010-03        | CP-47 | CP-100149 | 3007 | 1   | UE requirements in the absence of P-CSCF support of end to access edge security                                     | 9.2.0 | 9.3.0 | C1-100202 |
| 2010-03        | CP-47 | CP-100149 | 3008 | 1   | Profile additions for end to access edge security   | 9.2.0 | 9.3.0 | C1-100203 |
| 2010-03        | CP-47 | CP-100149 | 3009 | 1   | Coverage of media security in the security introduction   | 9.2.0 | 9.3.0 | C1-100204 |
| 2010-03        | CP-47 | CP-100151 | 3010 | 1   | Making the E-CSCF responsible for the domain of incoming Request-URI  | 9.2.0 | 9.3.0 | C1-100230 |
| 2010-03        | CP-47 | CP-100151 | 3011 | 1   | Usage of P-Charging-Vector header within the emergency call architecture  | 9.2.0 | 9.3.0 | C1-100199 |
| 2010-03        | CP-47 | CP-100151 | 3013 | 1   | Delivery of location by the E-CSCF  | 9.2.0 | 9.3.0 | C1-100159 |
| 2010-03        | CP-47 | CP-100151 | 3014 | 2   | Structure of reference identifier   | 9.2.0 | 9.3.0 | C1-100941 |
| 2010-03        | CP-47 | CP-100151 | 3015 | 1   | Handling of editor's note on subscribing to all dialogs   | 9.2.0 | 9.3.0 | C1-100160 |
| 2010-03        | CP-47 | CP-100109 | 3017 |     | Resolution of editor's notes related to PRIOR   | 9.2.0 | 9.3.0 | C1-100208 |
| 2010-03        | CP-47 | CP-100230 | 3019 | 1   | Removal of editor's notes relating to learning of trust domain boundaries and information saved during registration | 9.2.0 | 9.3.0 | -         |
| 2010-03        | CP-47 | CP-100135 | 3020 | 1   | Correcting IP-CAN documentation   | 9.2.0 | 9.3.0 | C1-100944 |
| 2010-03        | CP-47 | CP-100153 | 3024 |     | P-CSCF Note correction  | 9.2.0 | 9.3.0 | C1-100339 |
| 2010-03        | CP-47 | CP-100153 | 3025 |     | Authentication-Info header field  | 9.2.0 | 9.3.0 | C1-100340 |
| 2010-03        | CP-47 | CP-100153 | 3026 | 4   | DTMF Info Package definition  | 9.2.0 | 9.3.0 | C1-101119 |
| 2010-03        | CP-47 | CP-100110 | 3028 |     | Removal of editor's note: 199 (Early Dialog Terminated) option-tag  | 9.2.0 | 9.3.0 | C1-100366 |
| 2010-03        | CP-47 | CP-100111 | 3031 |     | Removal of editor's note: Annex K NAT traversal   | 9.2.0 | 9.3.0 | C1-100369 |
| 2010-03        | CP-47 | CP-100107 | 3035 |     | Closure of SAES related editor's notes  | 9.2.0 | 9.3.0 | C1-100419 |
| 2010-03        | CP-47 | CP-100117 | 3037 |     | Addressing editor's notes relating to NASS bundled authentication   | 9.2.0 | 9.3.0 | C1-100421 |
| 2010-03        | CP-47 | CP-100110 | 3039 |     | Removal of editor's notes relating to emergency call  | 9.2.0 | 9.3.0 | C1-100423 |
| 2010-03        | CP-47 | CP-100110 | 3043 |     | Removal of outstanding Editor's note on IOI   | 9.2.0 | 9.3.0 | C1-100436 |

| Change history |       |           |      |     |  |       |       |           |
|----------------|-------|-----------|------|-----|--|-------|-------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old   | New   | WG doc    |
| 2010-03        | CP-47 | CP-100107 | 3045 |     | Incorrect NAS message in Annex L   | 9.2.0 | 9.3.0 | C1-100454 |
| 2010-03        | CP-47 | CP-100135 | 3048 | 2   | Delete EN pertaining to RFC 4117   | 9.2.0 | 9.3.0 | C1-101156 |
| 2010-03        | CP-47 | CP-100122 | 3053 |     | Incorrect trigger in I-CSCF for restoration procedures                                 | 9.2.0 | 9.3.0 | C1-100462 |
| 2010-03        | CP-47 | CP-100112 | 3054 | 1   | Clean up editor's notes on subscription to debug event package                         | 9.2.0 | 9.3.0 | C1-100983 |
| 2010-03        | CP-47 | CP-100149 | 3055 | 1   | Exchanging media plane security capabilities at registration                           | 9.2.0 | 9.3.0 | C1-100971 |
| 2010-03        | CP-47 | CP-100218 | 3056 | 2   | Profile table changes for exchanging media plane security capabilities at registration | 9.2.0 | 9.3.0 | -         |
| 2010-03        | CP-47 | CP-100153 | 3057 | 1   | Corrections to profile table entries related to security agreement                     | 9.2.0 | 9.3.0 | C1-100973 |
| 2010-03        | CP-47 | CP-100110 | 3059 | 1   | Inclusion of draft alert-urns for INVITE Responses                                     | 9.2.0 | 9.3.0 | C1-100954 |
| 2010-03        | CP-47 | CP-100119 | 3063 |     | Reference update of draft-ietf-mediactrl-vxml  | 9.2.0 | 9.3.0 | C1-100518 |
| 2010-03        | CP-47 | CP-100118 | 3065 | 1   | Address the UUS related Editor's Note  | 9.2.0 | 9.3.0 | C1-100986 |
| 2010-03        | CP-47 | CP-100110 | 3069 | 1   | Correcting missing reference   | 9.2.0 | 9.3.0 | C1-100991 |
| 2010-03        | CP-47 | CP-100153 | 3072 | 4   | Session ID profile table alignment   | 9.2.0 | 9.3.0 | C1-101176 |
| 2010-03        | CP-47 | CP-100105 | 3075 | 1   | Annex A/ Fixing of missing status support in Tables                                    | 9.2.0 | 9.3.0 | C1-100982 |
| 2010-03        | CP-47 | CP-100105 | 3078 |     | Annex A/ P-Media-Authorization support   | 9.2.0 | 9.3.0 | C1-100666 |
| 2010-03        | CP-47 | CP-100105 | 3081 |     | Annex A / integration of resource management and SIP                                   | 9.2.0 | 9.3.0 | C1-100670 |
| 2010-03        | CP-47 | CP-100247 | 3082 | 2   | Additional routeing capabilities   | 9.2.0 | 9.3.0 | -         |
| 2010-03        | CP-47 | CP-100138 | 3083 | 3   | P-CSCF Restoration Procedures  | 9.2.0 | 9.3.0 | C1-101262 |
| 2010-03        | CP-47 | CP-100110 | 3086 |     | New version of IETF draft-yu-tel-dai   | 9.2.0 | 9.3.0 | C1-100684 |
| 2010-03        | CP-47 | CP-100110 | 3092 |     | Abnormal Digest procedures fix   | 9.2.0 | 9.3.0 | C1-100692 |
| 2010-03        | CP-47 | CP-100128 | 3094 |     | IMDN reference update  | 9.2.0 | 9.3.0 | C1-100694 |
| 2010-03        | CP-47 | CP-100140 | 3095 | 1   | I4 applicability and EATF functionality  | 9.2.0 | 9.3.0 | C1-100940 |
| 2010-03        | CP-47 | CP-100153 | 3096 |     | Failure of GPRS and EPS resource reservation   | 9.2.0 | 9.3.0 | C1-100703 |
| 2010-03        | CP-47 | CP-100142 | 3097 | 3   | Addition of Dialog Event package to profile tables in support of Inter-UE transfer     | 9.2.0 | 9.3.0 | C1-101162 |
| 2010-03        | CP-47 | CP-100151 | 3098 |     | Correction of reference to RFC 4235  | 9.2.0 | 9.3.0 | C1-100966 |
| 2010-03        | CP-47 | CP-100144 | 3099 |     | Emergency call clarifications in the absence of registration                           | 9.2.0 | 9.3.0 | C1-100774 |
| 2010-03        | CP-47 | CP-100110 | 3101 |     | Correct authentication and registration referencing for emergency registration         | 9.2.0 | 9.3.0 | C1-100805 |
| 2010-03        | CP-47 | CP-100107 | 3103 |     | P-Access-Network-Info correction for LTE   | 9.2.0 | 9.3.0 | C1-100808 |
| 2010-03        | CP-47 | CP-100104 | 3106 |     | Update reference for draft-patel-ecrit-sos-parameter                                   | 9.2.0 | 9.3.0 | C1-100811 |
| 2010-03        | CP-47 | CP-100216 | 3033 | 2   | Updating of SAES related references  | 9.2.0 | 9.3.0 | -         |
| 2010-03        | CP-47 |           |      |     | Editorial correction   | 9.3.0 | 9.3.1 | -         |
| 2010-06        | CP-48 | CP-100364 | 3012 | 3   | Completion of dialog event package usage   | 9.3.1 | 9.4.0 | C1-101860 |

| Change history |       |           |      |     |  |        |        |           |
|----------------|-------|-----------|------|-----|--|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old    | New    | WG doc    |
| 2010-06        | CP-48 | CP-100363 | 3118 | 1   | Profile table changes for SDES media plane security role                   | 9.3.1  | 9.4.0  | C1-101889 |
| 2010-06        | CP-48 | CP-100363 | 3119 |     | Using SDES cryptro attribute   | 9.3.1  | 9.4.0  | C1-101395 |
| 2010-06        | CP-48 | CP-100346 | 3121 |     | Wrong requirements for ICS MSC in profile tables                           | 9.3.1  | 9.4.0  | C1-101399 |
| 2010-06        | CP-48 | CP-100337 | 3129 |     | Reference updates  | 9.3.1  | 9.4.0  | C1-101472 |
| 2010-06        | CP-48 | CP-100359 | 3130 | 1   | norefersub corrections   | 9.3.1  | 9.4.0  | C1-101859 |
| 2010-06        | CP-48 | CP-100364 | 3131 |     | Charging tidyup  | 9.3.1  | 9.4.0  | C1-101487 |
| 2010-06        | CP-48 | CP-100359 | 3136 | 1   | MSC Server assisted mid-call feature - conferencing                        | 9.3.1  | 9.4.0  | C1-102032 |
| 2010-06        | CP-48 | CP-100340 | 3142 | 1   | RFC4694 for IBCF   | 9.3.1  | 9.4.0  | C1-101814 |
| 2010-06        | CP-48 | CP-100364 | 3148 |     | 3xx response replaced by response  | 9.3.1  | 9.4.0  | C1-101584 |
| 2010-06        | CP-48 | CP-100340 | 3151 | 1   | Use of P-Served-User header field in user location procedure               | 9.3.1  | 9.4.0  | C1-101812 |
| 2010-06        | CP-48 | CP-100340 | 3155 | 2   | IBCF and Content-Disposition   | 9.3.1  | 9.4.0  | C1-102031 |
| 2010-06        | CP-48 | CP-100351 | 3158 | 1   | Addition of MSRP SDP a=path attribute                                      | 9.3.1  | 9.4.0  | C1-101820 |
| 2010-06        | CP-48 | CP-100363 | 3161 | 1   | Roles relating to media plane security                                     | 9.3.1  | 9.4.0  | C1-101890 |
| 2010-06        | CP-48 | CP-100354 | 3162 | 2   | IMS available  | 9.3.1  | 9.4.0  | C1-102103 |
| 2010-06        | CP-48 | CP-100367 | 3040 | 1   | Identifying an emergency call at the P-CSCF                                | 9.4.0  | 10.0.0 | C1-101504 |
| 2010-06        | CP-48 | CP-100367 | 3110 |     | Handling of Privacy header   | 9.4.0  | 10.0.0 | C1-101838 |
| 2010-06        | CP-48 | CP-100367 | 3113 | 2   | S-CSCF triggering of Additional Routeing capability                        | 9.4.0  | 10.0.0 | C1-102042 |
| 2010-06        | CP-48 | CP-100367 | 3114 | 2   | xPON access type values in P-Access-Network-Info                           | 9.4.0  | 10.0.0 | C1-102043 |
| 2010-06        | CP-48 | CP-100367 | 3116 | 1   | Digit manipulation   | 9.4.0  | 10.0.0 | C1-101843 |
| 2010-06        | CP-48 | CP-100371 | 3124 | 1   | Digest authentication without Authorization header                         | 9.4.0  | 10.0.0 | C1-102012 |
| 2010-06        | CP-48 | CP-100367 | 3126 | 1   | Corrections for NASS-Bundled authentication                                | 9.4.0  | 10.0.0 | C1-101844 |
| 2010-06        | CP-48 | CP-100367 | 3134 |     | Miscellaneous editorial issues   | 9.4.0  | 10.0.0 | C1-101503 |
| 2010-06        | CP-48 | CP-100371 | 3137 |     | Usage of "trusted node authentication"                                     | 9.4.0  | 10.0.0 | C1-101509 |
| 2010-06        | CP-48 | CP-100367 | 3146 | 1   | Annex A, Table A.4, item 2C, reference update                              | 9.4.0  | 10.0.0 | C1-101845 |
| 2010-09        | CP-49 | CP-100510 | 3168 | 3   | Outbound reregistration at P-CSCF  | 10.0.0 | 10.1.0 | C1-102822 |
| 2010-09        | CP-49 | CP-100500 | 3171 | 3   | Initial registration for GPRS-IMS at S-CSCF                                | 10.0.0 | 10.1.0 | C1-102848 |
| 2010-09        | CP-49 | CP-100511 | 3172 | 5   | Privacy protection in IBCF   | 10.0.0 | 10.1.0 | C1-103526 |
| 2010-09        | CP-49 | CP-100639 | 3176 | 3   | Alignment with RFC 5552  | 10.0.0 | 10.1.0 | -         |
| 2010-09        | CP-49 | CP-100511 | 3178 | 6   | User-related policy data enforcement by the P-CSCF                         | 10.0.0 | 10.1.0 | C1-103517 |
| 2010-09        | CP-49 | CP-100640 | 3180 | 3   | Handling of aliases URIs   | 10.0.0 | 10.1.0 | -         |
| 2010-09        | CP-49 | CP-100641 | 3181 | 3   | Structure of the Request URI sent by a UE                                  | 10.0.0 | 10.1.0 | -         |
| 2010-09        | CP-49 | CP-100481 | 3188 | 2   | Home network check for (E)UTRAN access                                     | 10.0.0 | 10.1.0 | C1-103041 |
| 2010-09        | CP-49 | CP-100482 | 3196 | 1   | Updates to references pertaining to Internet Drafts for tel URI parameters | 10.0.0 | 10.1.0 | C1-102676 |

| Change history |       |           |      |     |   |        |        |           |
|----------------|-------|-----------|------|-----|---|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old    | New    | WG doc    |
| 2010-09        | CP-49 | CP-100519 | 3197 | 1   | Usage of alternative P-CSCF address during registration                                 | 10.0.0 | 10.1.0 | C1-102631 |
| 2010-09        | CP-49 | CP-100496 | 3198 | 8   | Mandate registration with IMS in order to receive audio/voice services                  | 10.0.0 | 10.1.0 | C1-103536 |
| 2010-09        | CP-49 | CP-100510 | 3200 |     | Annex A, Reason header  | 10.0.0 | 10.1.0 | C1-102448 |
| 2010-09        | CP-49 | CP-100652 | 3205 | 3   | Emergency registration in HPLMN   | 10.0.0 | 10.1.0 | -         |
| 2010-09        | CP-49 | CP-100486 | 3209 | 1   | Keep-alive corrections  | 10.0.0 | 10.1.0 | C1-102624 |
| 2010-09        | CP-49 | CP-100511 | 3211 | 4   | Passing policy with subscription information to UE and P-CSCF                           | 10.0.0 | 10.1.0 | C1-103504 |
| 2010-09        | CP-49 | CP-100486 | 3214 | 1   | Wildcarded identity AVP correction  | 10.0.0 | 10.1.0 | C1-102685 |
| 2010-09        | CP-49 | CP-100486 | 3217 |     | Subclause reference correction  | 10.0.0 | 10.1.0 | C1-102492 |
| 2010-09        | CP-49 | CP-100483 | 3221 |     | Update of draft-rosenberg-sip-app-media-tag reference                                   | 10.0.0 | 10.1.0 | C1-102532 |
| 2010-09        | CP-49 | CP-100511 | 3222 | 3   | Location number   | 10.0.0 | 10.1.0 | C1-103543 |
| 2010-09        | CP-49 | CP-100487 | 3226 |     | Updates to references pertaining to Internet Drafts for tel URI parameters              | 10.0.0 | 10.1.0 | C1-102679 |
| 2010-09        | CP-49 | CP-100511 | 3236 | 2   | Insertion of IMS access gateway by P-CSCF   | 10.0.0 | 10.1.0 | C1-103518 |
| 2010-09        | CP-49 | CP-100511 | 3237 | 4   | Enforcement of P-Early-Media indication by P-CSCF                                       | 10.0.0 | 10.1.0 | C1-103544 |
| 2010-09        | CP-49 | CP-100508 | 3239 |     | EN pertaining to Media Plane Security   | 10.0.0 | 10.1.0 | C1-103039 |
| 2010-09        | CP-49 | CP-100481 | 3243 | 2   | Detecting valid emergency identifiers   | 10.0.0 | 10.1.0 | C1-103542 |
| 2010-09        | CP-49 | CP-100501 | 3245 | 2   | Emergency PDN connection usage control in P-CSCF  | 10.0.0 | 10.1.0 | C1-103513 |
| 2010-09        | CP-49 | CP-100510 | 3249 | 1   | IBCF procedures for SIP message   | 10.0.0 | 10.1.0 | C1-103382 |
| 2010-09        | CP-49 | CP-100519 | 3250 | 2   | Indicating wildcarded IMPU in reg-event   | 10.0.0 | 10.1.0 | C1-103528 |
| 2010-09        | CP-49 | CP-100501 | 3252 | 1   | Wildcarded Identities handling  | 10.0.0 | 10.1.0 | C1-103354 |
| 2010-09        | CP-49 | CP-100481 | 3256 | 2   | Correction of Stage 3 misalignment with Stage 1 and Stage 2 on use of SIP 380 response. | 10.0.0 | 10.1.0 | C1-103389 |
| 2010-09        | CP-49 | CP-100519 | 3257 | 3   | SigComp disabling   | 10.0.0 | 10.1.0 | C1-103530 |
| 2010-09        | CP-49 | CP-100486 | 3258 | 2   | Ensuring PSAP receives correctly formatted request                                      | 10.0.0 | 10.1.0 | C1-103568 |
| 2010-09        | CP-49 | CP-100486 | 3261 | 1   | Mandate registration with IMS in order to receive audio/voice services                  | 10.0.0 | 10.1.0 | C1-103508 |
| 2010-12        | CP-50 | CP-100843 | 3305 | 2   | SRVCC enhancements - ATCF invocation  | 10.1.0 | 10.2.0 | C1-104362 |
| 2010-12        | CP-50 | CP-100728 | 3267 | 1   | Protected AKA registration at S-CSCF  | 10.1.0 | 10.2.0 | C1-104197 |
| 2010-12        | CP-50 | CP-100728 | 3270 | 1   | Protected Digest registration at S-CSCF   | 10.1.0 | 10.2.0 | C1-104300 |
| 2010-12        | CP-50 | CP-100728 | 3273 | 2   | Unprotected registration at S-CSCF  | 10.1.0 | 10.2.0 | C1-104370 |
| 2010-12        | CP-50 | CP-100750 | 3278 |     | Supported header field corrected  | 10.1.0 | 10.2.0 | C1-103619 |
| 2010-12        | CP-50 | CP-100728 | 3281 | 1   | Update reference  | 10.1.0 | 10.2.0 | C1-104310 |
| 2010-12        | CP-50 | CP-100725 | 3285 |     | Correcting mixed references in IBCF   | 10.1.0 | 10.2.0 | C1-103761 |
| 2010-12        | CP-50 | CP-100728 | 3288 | 3   | Conference and IBCF IMS_ALG and removal of an Editor's note.                            | 10.1.0 | 10.2.0 | C1-105071 |

| Change history |       |           |      |     |  |        |        |           |
|----------------|-------|-----------|------|-----|--|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old    | New    | WG doc    |
| 2010-12        | CP-50 | CP-100735 | 3291 |     | Correcting errors in S-CSCF restoration procedures                                 | 10.1.0 | 10.2.0 | C1-103773 |
| 2010-12        | CP-50 | CP-100728 | 3301 |     | Incorrect sequence of steps in P-CSCF  | 10.1.0 | 10.2.0 | C1-104316 |
| 2010-12        | CP-50 | CP-100723 | 3304 |     | Emergency registration and normal registration                                     | 10.1.0 | 10.2.0 | C1-104183 |
| 2010-12        | CP-50 | CP-100738 | 3314 | 1   | Updating IMEI URN draft reference  | 10.1.0 | 10.2.0 | C1-104328 |
| 2010-12        | CP-50 | CP-100721 | 3319 |     | IETF reference updates   | 10.1.0 | 10.2.0 | C1-103921 |
| 2010-12        | CP-50 | CP-100722 | 3324 |     | IETF reference updates   | 10.1.0 | 10.2.0 | C1-103926 |
| 2010-12        | CP-50 | CP-100726 | 3328 |     | IETF reference updates   | 10.1.0 | 10.2.0 | C1-103936 |
| 2010-12        | CP-50 | CP-100728 | 3331 |     | IETF reference updates   | 10.1.0 | 10.2.0 | C1-104337 |
| 2010-12        | CP-50 | CP-100728 | 3334 |     | EN removal: Retry-After Header field value in 503 response                         | 10.1.0 | 10.2.0 | C1-103955 |
| 2010-12        | CP-50 | CP-100728 | 3340 |     | EN removal: Network inserted codecs  | 10.1.0 | 10.2.0 | C1-103961 |
| 2010-12        | CP-50 | CP-100723 | 3344 | 1   | Further modifications required to SIP 380 response to remove new requirements.     | 10.1.0 | 10.2.0 | C1-104187 |
| 2010-12        | CP-50 | CP-100864 | 3345 | 4   | Inclusion of IMEI in the sip.instance of the initial SIP-Register request          | 10.1.0 | 10.2.0 | C1-105086 |
| 2010-12        | CP-50 | CP-100733 | 3348 |     | Handling of editor's note relating to private network traffic breakout and breakin | 10.1.0 | 10.2.0 | C1-103984 |
| 2010-12        | CP-50 | CP-100726 | 3354 | 2   | Inclusion of file transfer attributes  | 10.1.0 | 10.2.0 | C1-104986 |
| 2010-12        | CP-50 | CP-100752 | 3355 | 2   | IBCF and 3xx responses   | 10.1.0 | 10.2.0 | C1-104595 |
| 2010-12        | CP-50 | CP-100752 | 3356 |     | Non E.164 Tel URI conversion failure   | 10.1.0 | 10.2.0 | C1-104464 |
| 2010-12        | CP-50 | CP-100750 | 3357 | 2   | max-time and base-time parameters provision  | 10.1.0 | 10.2.0 | C1-105207 |
| 2010-12        | CP-50 | CP-100752 | 3358 |     | reference correction   | 10.1.0 | 10.2.0 | C1-104466 |
| 2010-12        | CP-50 | CP-100728 | 3361 | 1   | AKA registration at S-CSCF   | 10.1.0 | 10.2.0 | C1-104991 |
| 2010-12        | CP-50 | CP-100728 | 3364 | 2   | Autentication already performed  | 10.1.0 | 10.2.0 | C1-105203 |
| 2010-12        | CP-50 | CP-100728 | 3367 | 1   | Digest registration at S-CSCF  | 10.1.0 | 10.2.0 | C1-104997 |
| 2010-12        | CP-50 | CP-100728 | 3370 | 1   | Bundle registration  | 10.1.0 | 10.2.0 | C1-105000 |
| 2010-12        | CP-50 | CP-100720 | 3377 | 1   | Codec and DTMF correction  | 10.1.0 | 10.2.0 | C1-104980 |
| 2010-12        | CP-50 | CP-100728 | 3380 |     | Definition: multiple registrations   | 10.1.0 | 10.2.0 | C1-104535 |
| 2010-12        | CP-50 | CP-100871 | 3383 | 1   | Reference update: draft-ietf-sipcore-199   | 10.1.0 | 10.2.0 | -         |
| 2010-12        | CP-50 | CP-100724 | 3387 |     | Reference update: draft-ietf-sipcore-keep  | 10.1.0 | 10.2.0 | C1-104547 |
| 2010-12        | CP-50 | CP-100864 | 3388 | 2   | Modifications to priority handling in support of MPS                               | 10.1.0 | 10.2.0 | C1-105095 |
| 2010-12        | CP-50 | CP-100885 | 3389 | 3   | Updating the restoration procedure definition                                      | 10.1.0 | 10.2.0 | -         |
| 2010-12        | CP-50 | CP-100752 | 3390 |     | Adding RFC 5318 to major capabilities tables                                       | 10.1.0 | 10.2.0 | C1-105226 |
| 2010-12        | CP-50 | CP-100728 | 3393 | 1   | Handling of the isfocus media feature tag in P-CSCF                                | 10.1.0 | 10.2.0 | C1-105003 |
| 2010-12        | CP-50 | CP-100752 | 3394 |     | Annex A, Table A.4, item 29+72 and Table A.4A, prerequisite                        | 10.1.0 | 10.2.0 | C1-104618 |
| 2010-12        | CP-50 | CP-100728 | 3397 |     | "ob" parameter in case of no registration  | 10.1.0 | 10.2.0 | C1-105006 |
| 2010-12        | CP-50 | CP-100728 | 3401 | 2   | Addition of Target-Dialog header and capability in Annex A                         | 10.1.0 | 10.2.0 | C1-105074 |

| Change history |       |           |      |     |   |        |        |           |
|----------------|-------|-----------|------|-----|---|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old    | New    | WG doc    |
| 2010-12        | CP-50 | CP-100766 | 3405 | 2   | Alternative emergency session handling in non-roaming cases (P-CSCF)                  | 10.1.0 | 10.2.0 | C1-105052 |
| 2010-12        | CP-50 | CP-100766 | 3406 | 2   | Alternative emergency session handling in non-roaming cases (S-CSCF)                  | 10.1.0 | 10.2.0 | C1-105053 |
| 2010-12        | CP-50 | CP-100766 | 3407 |     | Alternative emergency session handling in non-roaming cases (E-CSCF)                  | 10.1.0 | 10.2.0 | C1-104682 |
| 2010-12        | CP-50 | CP-100749 | 3409 |     | Removal of erroneous passing on of IOI value to PSAP                                  | 10.1.0 | 10.2.0 | C1-104718 |
| 2010-12        | CP-50 | CP-100766 | 3411 |     | Additions to E-CSCF functionality for IESE  | 10.1.0 | 10.2.0 | C1-104721 |
| 2010-12        | CP-50 | CP-100766 | 3412 |     | IBCF detection and routeing of emergency call   | 10.1.0 | 10.2.0 | C1-104722 |
| 2010-12        | CP-50 | CP-100864 | 3413 | 3   | Introduction to priority schemes in the IM CN subsystem                               | 10.1.0 | 10.2.0 | C1-105221 |
| 2010-12        | CP-50 | CP-100766 | 3414 | 1   | Addition to introductory clauses in support of IESE                                   | 10.1.0 | 10.2.0 | C1-104974 |
| 2010-12        | CP-50 | CP-100725 | 3415 | 1   | Correction of the usage for type 3 IOI  | 10.1.0 | 10.2.0 | C1-105051 |
| 2010-12        | CP-50 | CP-100864 | 3425 | 2   | P-CSCF behaviour for insufficient bandwidth   | 10.1.0 | 10.2.0 | C1-105058 |
| 2010-12        | CP-50 | CP-100752 | 3416 | 1   | Text corrections  | 10.1.0 | 10.2.0 | C1-104969 |
| 2010-12        | CP-50 | CP-100727 | 3420 |     | Update of IETF reference  | 10.1.0 | 10.2.0 | C1-104842 |
| 2011-03        | CP-51 | CP-110181 | 3371 | 4   | Sending of location information from LRF to E-CSCF                                    | 10.2.0 | 10.3.0 | C1-110671 |
| 2011-03        | CP-51 | CP-110181 | 3429 | 2   | Response code in Reason header field  | 10.2.0 | 10.3.0 | C1-110659 |
| 2011-03        | CP-51 | CP-110164 | 3432 | 1   | UE initiated deregistration   | 10.2.0 | 10.3.0 | C1-110581 |
| 2011-03        | CP-51 | CP-110181 | 3433 |     | Other databases   | 10.2.0 | 10.3.0 | C1-110010 |
| 2011-03        | CP-51 | CP-110181 | 3434 | 1   | Clarification of possible triggers for network-initiated reauthentication             | 10.2.0 | 10.3.0 | C1-110560 |
| 2011-03        | CP-51 | CP-110161 | 3435 | 6   | Update to IMS registration procedures due to USAT initiated Refresh for ISIM/USIM EFs | 10.2.0 | 10.3.0 | C1-111511 |
| 2011-03        | CP-51 | CP-110184 | 3436 | 1   | Optimal Media Routeing – SDP attribute syntax definition                              | 10.2.0 | 10.3.0 | C1-110558 |
| 2011-03        | CP-51 | CP-110184 | 3437 | 1   | Update SDP profile table for Optimal Media Routeing                                   | 10.2.0 | 10.3.0 | C1-110559 |
| 2011-03        | CP-51 | CP-110196 | 3439 | 1   | Modifications to S-CSCF procedures in support of MPS                                  | 10.2.0 | 10.3.0 | C1-110562 |
| 2011-03        | CP-51 | CP-110196 | 3440 | 1   | Modifications to P-CSCF and IBCF procedures in support of MPS                         | 10.2.0 | 10.3.0 | C1-110563 |
| 2011-03        | CP-51 | CP-110201 | 3441 | 1   | Select E-CSCF upon S-SCSF failure   | 10.2.0 | 10.3.0 | C1-110557 |
| 2011-03        | CP-51 | CP-110158 | 3445 | 1   | Correct P-CSCF handling of requests for emergency services with Route header fields   | 10.2.0 | 10.3.0 | C1-110567 |
| 2011-03        | CP-51 | CP-110196 | 3450 |     | Clarification on P-CSCF behaviour in case of insufficient bandwidth                   | 10.2.0 | 10.3.0 | C1-110180 |
| 2011-03        | CP-51 | CP-110166 | 3453 | 2   | New Reference for Alert-URN   | 10.2.0 | 10.3.0 | C1-111349 |
| 2011-03        | CP-51 | CP-110187 | 3457 | 5   | Explicit Congestion Notification (ECN) for RTP over UDP                               | 10.2.0 | 10.3.0 | C1-111360 |
| 2011-03        | CP-51 | CP-110196 | 3458 | 4   | Clarify the P-CSCF restoration procedure  | 10.2.0 | 10.3.0 | C1-111271 |
| 2011-03        | CP-51 | CP-110164 | 3461 | 1   | Reference update: draft-ietf-mmusic-ice-tcp   | 10.2.0 | 10.3.0 | C1-110578 |

| Change history |       |           |      |     |   |        |        |           |
|----------------|-------|-----------|------|-----|---|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old    | New    | WG doc    |
| 2011-03        | CP-51 | CP-110164 | 3464 | 1   | Reference update: RFC 6086  | 10.2.0 | 10.3.0 | C1-110589 |
| 2011-03        | CP-51 | CP-110159 | 3468 |     | Reference update: draft-ietf-sipcore-keep   | 10.2.0 | 10.3.0 | C1-110267 |
| 2011-03        | CP-51 | CP-110164 | 3471 | 3   | P-CSCF Path SIP URI and IMS flow token correction   | 10.2.0 | 10.3.0 | C1-111283 |
| 2011-03        | CP-51 | CP-110196 | 3474 | 1   | Encoding of PANI for E-UTRAN  | 10.2.0 | 10.3.0 | C1-110442 |
| 2011-03        | CP-51 | CP-110196 | 3475 | 3   | Insertion of "orig" parameter by IBCF   | 10.2.0 | 10.3.0 | C1-110665 |
| 2011-03        | CP-51 | CP-110196 | 3479 | 5   | Removal of reference CPC and OLI Internet Draft   | 10.2.0 | 10.3.0 | C1-111329 |
| 2011-03        | CP-51 | CP-110158 | 3483 | 2   | Specifying "sos" URI parameter in 24.229  | 10.2.0 | 10.3.0 | C1-111087 |
| 2011-03        | CP-51 | CP-110196 | 3484 | 7   | Example of IMS Registration conditions, taking into account the network operator's preference for selection of the voice domain | 10.2.0 | 10.3.0 | C1-111270 |
| 2011-03        | CP-51 | CP-110181 | 3486 | 2   | Removal of Sigcomp disabling  | 10.2.0 | 10.3.0 | C1-111266 |
| 2011-03        | CP-51 | CP-110164 | 3489 |     | New registration  | 10.2.0 | 10.3.0 | C1-110842 |
| 2011-03        | CP-51 | CP-110309 | 3490 | 6   | Inclusion of MEID in the sip.instance of the SIP-Register request   | 10.2.0 | 10.3.0 | -         |
| 2011-03        | CP-51 | CP-110181 | 3491 | 1   | Disabling SigComp by default in E-UTRAN   | 10.2.0 | 10.3.0 | C1-111221 |
| 2011-03        | CP-51 | CP-110164 | 3495 | 1   | S-CSCF Service-Route SIP URI  | 10.2.0 | 10.3.0 | C1-111274 |
| 2011-03        | CP-51 | CP-110184 | 3496 | 4   | Introduction of OMR procedures in AS, MGCF and P-CSCF   | 10.2.0 | 10.3.0 | C1-111359 |
| 2011-03        | CP-51 | CP-110181 | 3497 |     | Removal of editor's note: different sets of policies for a user   | 10.2.0 | 10.3.0 | C1-111235 |
| 2011-03        | CP-51 | CP-110181 | 3498 |     | Removal of editor's note: additional policy elements  | 10.2.0 | 10.3.0 | C1-110939 |
| 2011-03        | CP-51 | CP-110164 | 3501 |     | Reference update and procedure correction: 199  | 10.2.0 | 10.3.0 | C1-111277 |
| 2011-03        | CP-51 | CP-110162 | 3502 | 1   | Contact header clarification  | 10.2.0 | 10.3.0 | C1-111240 |
| 2011-03        | CP-51 | CP-110160 | 3507 | 1   | MGCF procedure corrections related to SIP preconditions   | 10.2.0 | 10.3.0 | C1-111259 |
| 2011-03        | CP-51 | CP-110164 | 3510 |     | Erroneous row reference in Table A.50A  | 10.2.0 | 10.3.0 | C1-111000 |
| 2011-03        | CP-51 | CP-110164 | 3514 | 1   | Correction reference  | 10.2.0 | 10.3.0 | C1-111280 |
| 2011-03        | CP-51 | CP-110176 | 3517 | 2   | Correction to the header field indicating where the request comes from in E-CSCF procedures                                     | 10.2.0 | 10.3.0 | C1-111325 |
| 2011-03        | CP-51 | CP-110181 | 3519 | 1   | Editorial corrections to S-CSCF registration subclauses   | 10.2.0 | 10.3.0 | C1-111241 |
| 2011-03        | CP-51 | CP-110181 | 3520 | 3   | Clarification of authentication of 380 and 504 responses with multiple registration   | 10.2.0 | 10.3.0 | C1-111337 |
| 2011-03        | CP-51 | CP-110181 | 3521 | 1   | Provision of phone-context parameter value via MO   | 10.2.0 | 10.3.0 | C1-111245 |
| 2011-03        | CP-51 | CP-110010 | 3522 | 3   | P-CSCF graceful shutdown  | 10.2.0 | 10.3.0 | -         |
| 2011-06        | CP-52 | CP-110450 | 3532 | 1   | Reference update: 199   | 10.3.0 | 10.4.0 | C1-112024 |
| 2011-06        | CP-52 | CP-110445 | 3536 | 1   | Reference update: RFC 6223  | 10.3.0 | 10.4.0 | C1-112013 |
| 2011-06        | CP-52 | CP-110450 | 3539 |     | Annex A: RFC 6086 reference corrections   | 10.3.0 | 10.4.0 | C1-111556 |
| 2011-06        | CP-52 | CP-110468 | 3540 | 1   | Removal of Annex F.3  | 10.3.0 | 10.4.0 | C1-112015 |
| 2011-06        | CP-52 | CP-110468 | 3541 | 1   | Moving of P-CSCF ICE procedures (Annex K.3.2 and K.5.3)   | 10.3.0 | 10.4.0 | C1-112016 |



| Change history |       |           |      |     |   |        |        |           |
|----------------|-------|-----------|------|-----|---|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old    | New    | WG doc    |
| 2011-06        | CP-52 | CP-110468 | 3542 | 1   | Removal of Annex G  | 10.3.0 | 10.4.0 | C1-112014 |
| 2011-06        | CP-52 | CP-110468 | 3545 | 1   | S-CSCF-initiated session release                                  | 10.3.0 | 10.4.0 | C1-112025 |
| 2011-06        | CP-52 | CP-110450 | 3548 | 1   | Service-Route at the UE   | 10.3.0 | 10.4.0 | C1-112040 |
| 2011-06        | CP-52 | CP-110450 | 3551 | 1   | Service-Route at the P-CSCF                                       | 10.3.0 | 10.4.0 | C1-112043 |
| 2011-06        | CP-52 | CP-110450 | 3554 | 2   | Service-Route at the S-CSCF                                       | 10.3.0 | 10.4.0 | C1-112227 |
| 2011-06        | CP-52 | CP-110450 | 3557 | 1   | Path header field at the S-CSCF                                   | 10.3.0 | 10.4.0 | C1-112049 |
| 2011-06        | CP-52 | CP-110450 | 3560 | 1   | S-CSCF releasing the dialogs                                      | 10.3.0 | 10.4.0 | C1-112052 |
| 2011-06        | CP-52 | CP-110450 | 3563 | 1   | NOTIFY request  | 10.3.0 | 10.4.0 | C1-112028 |
| 2011-06        | CP-52 | CP-110450 | 3566 | 1   | Network Initiated deregistration at S-CSCF                        | 10.3.0 | 10.4.0 | C1-112031 |
| 2011-06        | CP-52 | CP-110450 | 3569 | 2   | Network Initiated deregistration at P-CSCF                        | 10.3.0 | 10.4.0 | C1-112223 |
| 2011-06        | CP-52 | CP-110450 | 3572 | 1   | Network Initiated deregistration at UE                            | 10.3.0 | 10.4.0 | C1-112037 |
| 2011-06        | CP-52 | CP-110468 | 3573 |     | UE initiated deregistration                                       | 10.3.0 | 10.4.0 | C1-111590 |
| 2011-06        | CP-52 | CP-110448 | 3578 | 1   | P-Access-Network-Info : ABNF correction                           | 10.3.0 | 10.4.0 | C1-112004 |
| 2011-06        | CP-52 | CP-110468 | 3579 | 1   | Moving of IBCF ICE procedures (Annex K.5.4)                       | 10.3.0 | 10.4.0 | C1-112017 |
| 2011-06        | CP-52 | CP-110531 | 3583 | 1   | SRVCC enhancements in Annex A                                     | 10.3.0 | 10.4.0 | -         |
| 2011-06        | CP-52 | CP-110469 | 3584 |     | ENs on P-CSCF invoking ATCF                                       | 10.3.0 | 10.4.0 | C1-111614 |
| 2011-06        | CP-52 | CP-110465 | 3585 | 1   | Inclusion of MEID in the sip.instance of the SIP-Register request | 10.3.0 | 10.4.0 | C1-112201 |
| 2011-06        | CP-52 | CP-110465 | 3586 | 1   | Clarification of scope of section 5.1.6 on Emergency Call         | 10.3.0 | 10.4.0 | C1-112089 |
| 2011-06        | CP-52 | CP-110447 | 3591 | 1   | Fraud prevention for deregistration for ICS                       | 10.3.0 | 10.4.0 | C1-112061 |
| 2011-06        | CP-52 | CP-110474 | 3596 | 2   | UICC Access to IMS  | 10.3.0 | 10.4.0 | C1-112249 |
| 2011-06        | CP-52 | CP-110447 | 3599 | 1   | Updating IMEI URN draft reference                                 | 10.3.0 | 10.4.0 | C1-112058 |
| 2011-06        | CP-52 | CP-110468 | 3602 | 2   | Insertion of "gated" parameter by the P-CSCF                      | 10.3.0 | 10.4.0 | C1-112231 |
| 2011-06        | CP-52 | CP-110451 | 3605 | 1   | Removal of dial around indicator                                  | 10.3.0 | 10.4.0 | C1-112235 |
| 2011-06        | CP-52 | CP-110477 | 3606 | 1   | OMR designation as media level attributes in profile              | 10.3.0 | 10.4.0 | C1-112096 |
| 2011-06        | CP-52 | CP-110472 | 3612 | 2   | Application server detection and routing of emergency call        | 10.3.0 | 10.4.0 | C1-112232 |
| 2011-06        | CP-52 | CP-110468 | 3613 | 1   | Removal of duplicate material in P-CSCF emergency call handling   | 10.3.0 | 10.4.0 | C1-112094 |
| 2011-06        | CP-52 | CP-110468 | 3622 |     | Miscellaneous 24.229 corrections                                  | 10.3.0 | 10.4.0 | C1-111949 |
| 2011-06        | CP-52 | CP-110521 | 3611 | 3   | Removal of repetition of IOI header field parameters              | 10.3.0 | 10.4.0 | -         |
| 2011-06        | CP-52 | CP-110535 | 3518 | 4   | Reference Location for Emergency Service                          | 10.4.0 | 11.0.0 | -         |
| 2011-09        | CP-53 | CP-110686 | 3624 | 1   | Reference update  | 11.0.0 | 11.1.0 | C1-112731 |
| 2011-09        | CP-53 | CP-110654 | 3633 | 3   | Correcting errors in S-CSCF restoration procedure                 | 11.0.0 | 11.1.0 | C1-113584 |
| 2011-09        | CP-53 | CP-110656 | 3641 | 2   | P-Profile-Key header field corrections in I-CSCF                  | 11.0.0 | 11.1.0 | C1-112915 |
| 2011-09        | CP-53 | CP-110693 | 3648 | 3   | Emergency session when IMS voice over PS is not supported         | 11.0.0 | 11.1.0 | C1-113170 |
| 2011-09        | CP-53 | CP-110666 | 3651 |     | EATF in Annex A   | 11.0.0 | 11.1.0 | C1-112512 |

| Change history |       |           |      |     |   |        |        |           |
|----------------|-------|-----------|------|-----|---|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old    | New    | WG doc    |
| 2011-09        | CP-53 | CP-110695 | 3657 | 2   | Correction on call initiation procedure at the MGCF   | 11.0.0 | 11.1.0 | C1-112945 |
| 2011-09        | CP-53 | CP-110686 | 3658 |     | Editorial corrections on SIP header field name  | 11.0.0 | 11.1.0 | C1-112519 |
| 2011-09        | CP-53 | CP-110689 | 3659 | 1   | Address the Editor's Note in RLI  | 11.0.0 | 11.1.0 | C1-112725 |
| 2011-09        | CP-53 | CP-110704 | 3665 | 3   | Additional IOI correction for SIP responses   | 11.0.0 | 11.1.0 | -         |
| 2011-09        | CP-53 | CP-110653 | 3669 | 1   | Replacement of draft-garcia-mmusic-sdp-misc-cap with draft-garcia-mmusic-sdp-miscellaneous-caps | 11.0.0 | 11.1.0 | C1-113294 |
| 2011-09        | CP-53 | CP-110686 | 3670 | 4   | Filtering of P-Associated-URI at P-CSCF   | 11.0.0 | 11.1.0 | C1-113440 |
| 2011-09        | CP-53 | CP-110674 | 3676 | 2   | Modification on roles of ATCF   | 11.0.0 | 11.1.0 | C1-112928 |
| 2011-09        | CP-53 | CP-110651 | 3683 | 1   | Emergency call – correction of requests covered at the P-CSCF                                   | 11.0.0 | 11.1.0 | C1-112832 |
| 2011-09        | CP-53 | CP-110658 | 3687 |     | IETF reference update   | 11.0.0 | 11.1.0 | C1-112647 |
| 2011-09        | CP-53 | CP-110681 | 3689 | 1   | Removal of "select an E-CSCF"   | 11.0.0 | 11.1.0 | C1-112754 |
| 2011-09        | CP-53 | CP-110686 | 3691 | 2   | Release of Media Bearers  | 11.0.0 | 11.1.0 | C1-112937 |
| 2011-09        | CP-53 | CP-110686 | 3693 | 2   | Network identified by IOI header field parameter  | 11.0.0 | 11.1.0 | C1-112960 |
| 2011-09        | CP-53 | CP-110648 | 3700 |     | "P-Visited-Network-ID" correction   | 11.0.0 | 11.1.0 | C1-113004 |
| 2011-09        | CP-53 | C1-110715 | 3701 | 2   | Emergency session handling correction   | 11.0.0 | 11.1.0 | -         |
| 2011-09        | CP-53 | CP-110681 | 3703 |     | Deletion of Editor's Note Concerning P-CSCF Dialstring Recognition                              | 11.0.0 | 11.1.0 | C1-113087 |
| 2011-09        | CP-53 | CP-110693 | 3707 | 1   | Emergency Session Setup – Incorrect Reference   | 11.0.0 | 11.1.0 | C1-113445 |
| 2011-09        | CP-53 | CP-110677 | 3713 | 2   | Policy passing when different policies are related to different IMPIs sharing an IMPU           | 11.0.0 | 11.1.0 | C1-113698 |
| 2011-09        | CP-53 | CP-110681 | 3715 |     | ENs on XML namespace registration   | 11.0.0 | 11.1.0 | C1-113176 |
| 2011-09        | CP-53 | CP-110656 | 3719 | 1   | Adding Call-Info to SUBSCRIBE in annex A  | 11.0.0 | 11.1.0 | C1-113529 |
| 2011-09        | CP-53 | CP-110653 | 3730 |     | Updating IMEI URN draft reference   | 11.0.0 | 11.1.0 | C1-113287 |
| 2011-09        | CP-53 | CP-110653 | 3732 | 2   | Including draft-holmberg-sipcore-proxy-feature  | 11.0.0 | 11.1.0 | C1-113594 |
| 2011-09        | CP-53 | CP-110687 | 3740 |     | Transit IOI principles  | 11.0.0 | 11.1.0 | C1-113595 |
| 2011-09        | CP-53 | CP-110681 | 3744 |     | Deletion of Editor's Note in 24.229 on authentication mechanism (Rel-10)                        | 11.0.0 | 11.1.0 | C1-113374 |
| 2011-09        | CP-53 | CP-110681 | 3746 | 1   | Deletion of Editor's Note in 24.229 on aor attribute (Rel-10)                                   | 11.0.0 | 11.1.0 | C1-113476 |
| 2011-09        | CP-53 | CP-110661 | 3758 |     | Deletion of Editor's Note in 24.229 on NASS error message (Rel-8)                               | 11.0.0 | 11.1.0 | C1-113388 |
| 2011-09        | CP-53 | CP-110686 | 3759 |     | Inter-operator identifier corrections   | 11.0.0 | 11.1.0 | C1-113392 |
| 2011-09        | CP-53 | CP-110736 | 3762 | 2   | Correction on EMC handling of S-CSCF  | 11.0.0 | 11.1.0 | -         |
| 2011-09        | CP-53 | CP-110690 | 3763 |     | 3GPP2 reference corrections   | 11.0.0 | 11.1.0 | C1-113396 |
| 2011-12        | CP-54 | CP-110887 | 3673 | 9   | "Default handling" triggering correction  | 11.1.0 | 11.2.0 | C1-115232 |
| 2011-12        | CP-54 | CP-110887 | 3766 | 3   | AS determination of the served user identity  | 11.1.0 | 11.2.0 | C1-114942 |
| 2011-12        | CP-54 | CP-110887 | 3771 |     | Editorial correction of the P-CSCF behavior for TCP connection                                  | 11.1.0 | 11.2.0 | C1-113821 |
| 2011-12        | CP-54 | CP-110873 | 3773 | 1   | Update draft-atarius-dispatch-meid-urn  | 11.1.0 | 11.2.0 | C1-114376 |

| Change history |       |           |      |     |  |        |        |           |
|----------------|-------|-----------|------|-----|--|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old    | New    | WG doc    |
| 2011-12        | CP-54 | CP-110887 | 3786 | 1   | Correction on conditional expression of Major Capabilities                                       | 11.1.0 | 11.2.0 | C1-114384 |
| 2011-12        | CP-54 | CP-110852 | 3790 | 4   | P-CSCF behaviour for emergency calls when failure occurs   | 11.1.0 | 11.2.0 | C1-115362 |
| 2011-12        | CP-54 | CP-110887 | 3794 | 3   | Adding missing handling in NOTIFY body for a registration event                                  | 11.1.0 | 11.2.0 | C1-114462 |
| 2011-12        | CP-54 | CP-110887 | 3803 | 1   | P-Profile-Key header field corrections in AS   | 11.1.0 | 11.2.0 | C1-114214 |
| 2011-12        | CP-54 | CP-110887 | 3807 | 1   | P-Profile-Key header field corrections in S-CSCF   | 11.1.0 | 11.2.0 | C1-114215 |
| 2011-12        | CP-54 | CP-110887 | 3809 |     | S-CSCF flow selection correction   | 11.1.0 | 11.2.0 | C1-114106 |
| 2011-12        | CP-54 | CP-110887 | 3810 |     | S-CSCF determining supported IP version by UE for media  | 11.1.0 | 11.2.0 | C1-114107 |
| 2011-12        | CP-54 | CP-110881 | 3812 | 3   | ICSI to visited network  | 11.1.0 | 11.2.0 | C1-115170 |
| 2011-12        | CP-54 | CP-110868 | 3819 | 1   | Removal of editor's notes relating to insertion of P-Access-Network-Info header field by a proxy | 11.1.0 | 11.2.0 | C1-114206 |
| 2011-12        | CP-54 | CP-110887 | 3820 |     | Editorial corrections on SIP header field name   | 11.1.0 | 11.2.0 | C1-114534 |
| 2011-12        | CP-54 | CP-110887 | 3821 | 1   | Addition of IEEE802.3ah to P-Access-Network-Info header  | 11.1.0 | 11.2.0 | C1-115154 |
| 2011-12        | CP-54 | CP-110887 | 3822 |     | Editorial correction on de-registration of emergency service                                     | 11.1.0 | 11.2.0 | C1-114536 |
| 2011-12        | CP-54 | CP-110856 | 3827 | 1   | Incorrect reference to RFC 5261  | 11.1.0 | 11.2.0 | C1-115009 |
| 2011-12        | CP-54 | CP-110873 | 3834 | 2   | proxy-feature I-D reference update   | 11.1.0 | 11.2.0 | C1-115288 |
| 2011-12        | CP-54 | CP-110861 | 3840 |     | Inclusion of media feature tag ASN.1 identifiers   | 11.1.0 | 11.2.0 | C1-114594 |
| 2011-12        | CP-54 | CP-110887 | 3845 |     | Record-Route reference correction  | 11.1.0 | 11.2.0 | C1-114600 |
| 2011-12        | CP-54 | CP-110887 | 3846 | 1   | Number of emergency registrations  | 11.1.0 | 11.2.0 | C1-115167 |
| 2011-12        | CP-54 | CP-110850 | 3850 | 2   | Reference update: Reason header in SIP responses   | 11.1.0 | 11.2.0 | C1-115274 |
| 2011-12        | CP-54 | CP-110887 | 3855 | 4   | Additional granularity for IMS Communication Service Identifier                                  | 11.1.0 | 11.2.0 | C1-115348 |
| 2011-12        | CP-54 | CP-110869 | 3857 |     | Correction UE handling compression   | 11.1.0 | 11.2.0 | C1-114687 |
| 2011-12        | CP-54 | CP-110880 | 3859 | 1   | Routing of emergency requests via S-CSCF   | 11.1.0 | 11.2.0 | C1-115178 |
| 2011-12        | CP-54 | CP-110887 | 3860 | 1   | S-CSCF terminating procedures  | 11.1.0 | 11.2.0 | C1-115155 |
| 2011-12        | CP-54 | CP-110873 | 3862 | 2   | Transcoding Control at the IMS-ALG in the P-CSCF and related ECN corrections.                    | 11.1.0 | 11.2.0 | C1-115340 |
| 2011-12        | CP-54 | CP-110887 | 3863 | 1   | T1 Timer value for MRFC  | 11.1.0 | 11.2.0 | C1-115158 |
| 2011-12        | CP-54 | CP-110881 | 3868 | 1   | Adding availability for SMS over IMS determination   | 11.1.0 | 11.2.0 | C1-114971 |
| 2011-12        | CP-54 | CP-110881 | 3869 | 1   | ICSI included by AS in Feature-Caps header field in terminating requests                         | 11.1.0 | 11.2.0 | C1-115171 |
| 2011-12        | CP-54 | CP-110881 | 3870 |     | Indicating Multimedia Telephony Application Server in Feature-Caps header field                  | 11.1.0 | 11.2.0 | C1-114779 |
| 2011-12        | CP-54 | CP-110865 | 3874 | 1   | 3GPP2 reference corrections  | 11.1.0 | 11.2.0 | C1-115192 |
| 2011-12        | CP-54 | CP-110887 | 3879 | 2   | Correction on MRFC handling when receiving an INVITE message                                     | 11.1.0 | 11.2.0 | C1-115235 |
| 2011-12        | CP-54 | CP-110885 | 3891 | 2   | Additional routing function behaviour for transit ioi  | 11.1.0 | 11.2.0 | C1-115231 |

| Change history |       |           |      |     |  |        |        |           |
|----------------|-------|-----------|------|-----|--|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old    | New    | WG doc    |
| 2011-12        | CP-54 | CP-110887 | 3892 | 2   | Clarification on I-CSCF routing procedure for incoming call with Request-URI in SIP URI format | 11.1.0 | 11.2.0 | C1-115252 |
| 2012-01        |       |           |      |     | Correction of formatting in tables of annex A  | 11.2.0 | 11.2.1 |           |
| 2012-03        | CP-55 | CP-120118 | 3835 | 4   | IPXS: Application invocation procedures  | 11.2.1 | 11.3.0 | C1-120849 |
| 2012-03        | CP-55 | CP-120165 | 3844 | 3   | Updating of UUS references   | 11.2.1 | 11.3.0 | -         |
| 2012-03        | CP-55 | CP-120096 | 3900 |     | Corrections on the conditions of MSRP SDP a=path attribute                                     | 11.2.1 | 11.3.0 | C1-120114 |
| 2012-03        | CP-55 | CP-120117 | 3901 |     | Addition of procedures in case of Fiber access network   | 11.2.1 | 11.3.0 | C1-120148 |
| 2012-03        | CP-55 | CP-120117 | 3902 |     | Removal of Editor's Note about access-info of P-Access-Network-Info header                     | 11.2.1 | 11.3.0 | C1-120149 |
| 2012-03        | CP-55 | CP-120124 | 3903 | 1   | ICSI to visited network - ENs  | 11.2.1 | 11.3.0 | C1-120778 |
| 2012-03        | CP-55 | CP-120117 | 3905 | 2   | S-CSCF behavior when the number of simultaneous registrations for the same UE is reached.      | 11.2.1 | 11.3.0 | C1-120880 |
| 2012-03        | CP-55 | CP-120117 | 3906 | 3   | P-CSCF address provided by OMA DM for fixed access (Annex E).                                  | 11.2.1 | 11.3.0 | C1-120906 |
| 2012-03        | CP-55 | CP-120124 | 3909 | 3   | Use of Contact Parameters in a 3XX Response from an LRF  | 11.2.1 | 11.3.0 | C1-120898 |
| 2012-03        | CP-55 | CP-120093 | 3916 | 1   | Geo-Redundancy Registration  | 11.2.1 | 11.3.0 | C1-120556 |
| 2012-03        | CP-55 | CP-120107 | 3918 | 2   | P-CSCF forwarding REGISTER when ATCF is used   | 11.2.1 | 11.3.0 | C1-120869 |
| 2012-03        | CP-55 | CP-120112 | 3920 |     | IMS-ALG in the P-CSCF is invoked for Transcoding Control                                       | 11.2.1 | 11.3.0 | C1-120212 |
| 2012-03        | CP-55 | CP-120117 | 3921 | 2   | P-Served-User to BGCF  | 11.2.1 | 11.3.0 | C1-120854 |
| 2012-03        | CP-55 | CP-120090 | 3928 | 1   | Location Conveyance: Reference update  | 11.2.1 | 11.3.0 | C1-120562 |
| 2012-03        | CP-55 | CP-120117 | 3933 | 1   | Location Conveyance: Location Forwarding to MGCF and PSAP                                      | 11.2.1 | 11.3.0 | C1-120563 |
| 2012-03        | CP-55 | CP-120112 | 3940 | 1   | Reference update: draft-holmberg-sipcore-proxy-feature   | 11.2.1 | 11.3.0 | C1-120619 |
| 2012-03        | CP-55 | CP-120112 | 3942 | 1   | UE usage of Feature-Caps   | 11.2.1 | 11.3.0 | C1-120617 |
| 2012-03        | CP-55 | CP-120124 | 3945 | 1   | GRUU: UE self-assigned GRUU  | 11.2.1 | 11.3.0 | C1-120766 |
| 2012-03        | CP-55 | CP-120116 | 3947 | 2   | IMS_IOI_CH input on IBCF behaviour   | 11.2.1 | 11.3.0 | C1-120848 |
| 2012-03        | CP-55 | CP-120115 | 3948 | 1   | GINI input on profile tables   | 11.2.1 | 11.3.0 | C1-120696 |
| 2012-03        | CP-55 | CP-120092 | 3957 | 1   | Updating references to IMEI URN and XML body handling drafts                                   | 11.2.1 | 11.3.0 | C1-120583 |
| 2012-03        | CP-55 | CP-120112 | 3960 | 1   | Removing contradictory statement from User initiated deregistration procedure                  | 11.2.1 | 11.3.0 | C1-120621 |
| 2012-03        | CP-55 | CP-120117 | 3961 |     | Editorial corrections  | 11.2.1 | 11.3.0 | C1-120321 |
| 2012-03        | CP-55 | CP-120124 | 3962 | 1   | Clarification on forking related issues  | 11.2.1 | 11.3.0 | C1-120768 |
| 2012-03        | CP-55 | CP-120115 | 3967 | 2   | Add general support for RFC 6140   | 11.2.1 | 11.3.0 | C1-120850 |
| 2012-03        | CP-55 | CP-120115 | 3968 | 2   | Add complex UE support for RFC 6140 mainline GIN registration functionality                    | 11.2.1 | 11.3.0 | C1-120851 |

| Change history |       |           |      |     |   |        |        |           |
|----------------|-------|-----------|------|-----|---|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old    | New    | WG doc    |
| 2012-03        | CP-55 | CP-120115 | 3969 | 2   | Add S-CSCF support for RFC 6140 mainline GIN registration functionality                               | 11.2.1 | 11.3.0 | C1-120852 |
| 2012-03        | CP-55 | CP-120119 | 3970 | 3   | Introduction of MRB functional entity   | 11.2.1 | 11.3.0 | C1-120896 |
| 2012-06        | CP-56 | CP-120299 | 3896 | 2   | Reference update for MIKEY_TICKET RFC   | 11.3.0 | 11.4.0 | C1-121104 |
| 2012-06        | CP-56 | CP-120314 | 3904 | 6   | P-Served-User and session case  | 11.3.0 | 11.4.0 | C1-122360 |
| 2012-06        | CP-56 | CP-120307 | 3946 | 2   | P-CSCF releasing the session when resource is lost  | 11.3.0 | 11.4.0 | C1-121545 |
| 2012-06        | CP-56 | CP-120307 | 3952 | 8   | Correcting procedure for propagating service profile update to the UE                                 | 11.3.0 | 11.4.0 | C1-122450 |
| 2012-06        | CP-56 | CP-120324 | 3971 | 6   | Addition of the transit and roaming function  | 11.3.0 | 11.4.0 | C1-122413 |
| 2012-06        | CP-56 | CP-120323 | 3975 | 4   | PANI header support of network provided location information  | 11.3.0 | 11.4.0 | C1-122508 |
| 2012-06        | CP-56 | CP-120323 | 3976 | 4   | Distribution of location information- AS procedures   | 11.3.0 | 11.4.0 | C1-122509 |
| 2012-06        | CP-56 | CP-120289 | 3983 |     | Correction on SDP Profile Status  | 11.3.0 | 11.4.0 | C1-121042 |
| 2012-06        | CP-56 | CP-120314 | 3984 | 1   | Editorial correction on SDP Profile Status  | 11.3.0 | 11.4.0 | C1-121540 |
| 2012-06        | CP-56 | CP-120286 | 3989 |     | GRUU: S-CSCF URI matching   | 11.3.0 | 11.4.0 | C1-121054 |
| 2012-06        | CP-56 | CP-120284 | 3993 | 1   | Reference update: draft-salud-alert-info-urns   | 11.3.0 | 11.4.0 | C1-121416 |
| 2012-06        | CP-56 | CP-120307 | 3997 | 2   | Restoration procedures missing in entry IBCF  | 11.3.0 | 11.4.0 | C1-122250 |
| 2012-06        | CP-56 | CP-120306 | 3998 | 2   | Missing emergency call procedure in S-CSCF  | 11.3.0 | 11.4.0 | C1-121658 |
| 2012-06        | CP-56 | CP-120324 | 4000 | 6   | Loopback routeing   | 11.3.0 | 11.4.0 | C1-122412 |
| 2012-06        | CP-56 | CP-120322 | 4005 | 1   | Removal of EN regarding PUI format  | 11.3.0 | 11.4.0 | C1-121529 |
| 2012-06        | CP-56 | CP-120303 | 4011 |     | Correcting implementation error, dai parameter  | 11.3.0 | 11.4.0 | C1-121178 |
| 2012-06        | CP-56 | CP-120307 | 4012 |     | E-CSCF handling of PAI in responses   | 11.3.0 | 11.4.0 | C1-121179 |
| 2012-06        | CP-56 | CP-120307 | 4013 |     | Editorial corrections to 24.229   | 11.3.0 | 11.4.0 | C1-121190 |
| 2012-06        | CP-56 | CP-120314 | 4018 | 1   | Correcting incorrect references in P-CSCF procedures when emergency call failure occurs               | 11.3.0 | 11.4.0 | C1-121406 |
| 2012-06        | CP-56 | CP-120314 | 4019 | 7   | Correcting IBCF and profile tables for use of 3GPP IM CN subsystem XML body in restoration procedures | 11.3.0 | 11.4.0 | C1-122415 |
| 2012-06        | CP-56 | CP-120322 | 4020 | 7   | Addition of GRUU procedures for RFC6140 procedures  | 11.3.0 | 11.4.0 | C1-122480 |
| 2012-06        | CP-56 | CP-120286 | 4025 | 1   | Correcting contradictory statements regarding GRUU handling by IBCF                                   | 11.3.0 | 11.4.0 | C1-121411 |
| 2012-06        | CP-56 | CP-120314 | 4026 | 2   | Transparent passing of contact feature tags by B2BUA AS   | 11.3.0 | 11.4.0 | C1-121719 |
| 2012-06        | CP-56 | CP-120307 | 4027 | 1   | Use of Contact Parameters in a 3XX Response from an LRF   | 11.3.0 | 11.4.0 | C1-121546 |
| 2012-06        | CP-56 | CP-120301 | 4030 | 1   | Reference update: draft-ietf-avtcore-ecn-for-rtp  | 11.3.0 | 11.4.0 | C1-122285 |
| 2012-06        | CP-56 | CP-120427 | 4031 | 2   | Update to reference titles in TS 24.229   | 11.3.0 | 11.4.0 | -         |
| 2012-06        | CP-56 | CP-120314 | 4032 | 1   | Transparency to GRUU of B2BUA AS  | 11.3.0 | 11.4.0 | C1-122369 |
| 2012-06        | CP-56 | CP-120314 | 4033 | 2   | Addressing potential abuse of 3xx responses   | 11.3.0 | 11.4.0 | C1-122414 |

| Change history |       |           |      |     |  |        |        |           |
|----------------|-------|-----------|------|-----|--|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old    | New    | WG doc    |
| 2012-06        | CP-56 | CP-120303 | 4038 | 2   | Correcting ambiguity in restoration procedures definitions   | 11.3.0 | 11.4.0 | C1-122445 |
| 2012-06        | CP-56 | CP-120307 | 4041 | 1   | Adding the related-icid in charging overview   | 11.3.0 | 11.4.0 | C1-122365 |
| 2012-06        | CP-56 | CP-120295 | 4045 |     | Updating of UUS references   | 11.3.0 | 11.4.0 | C1-121944 |
| 2012-06        | CP-56 | CP-120292 | 4049 |     | IETF reference update (mixer-control)  | 11.3.0 | 11.4.0 | C1-121948 |
| 2012-06        | CP-56 | CP-120290 | 4058 | 1   | Correction on profile of REFER request   | 11.3.0 | 11.4.0 | C1-122268 |
| 2012-06        | CP-56 | CP-120314 | 4059 |     | Contact header field parameter values  | 11.3.0 | 11.4.0 | C1-121970 |
| 2012-06        | CP-56 | CP-120314 | 4064 | 1   | Adding 3gpp body xml schema to archive   | 11.3.0 | 11.4.0 | C1-122372 |
| 2012-06        | CP-56 | CP-120314 | 4069 | 3   | New technology annex when using the EPC via WLAN to access IM CN subsystem   | 11.3.0 | 11.4.0 | C1-122513 |
| 2012-06        | CP-56 | CP-120290 | 4074 |     | Handling of EN relating to granularity of access class   | 11.3.0 | 11.4.0 | C1-122089 |
| 2012-06        | CP-56 | CP-120314 | 4075 | 2   | Provision of access-type values in the P-CSCF, and Support of network location reporting for IMS functionality over GxGxx interfaces | 11.3.0 | 11.4.0 | C1-122491 |
| 2012-06        | CP-56 | CP-120314 | 4076 | 2   | Correction to the technology annex when using I-WLAN to access IM CN subsystem   | 11.3.0 | 11.4.0 | C1-122486 |
| 2012-06        | CP-56 | CP-120314 | 4077 |     | P-CSCF handling UE port along with IP address during registration  | 11.3.0 | 11.4.0 | C1-122116 |
| 2012-06        | CP-56 | CP-120307 | 4079 | 2   | Use of Contact Parameters in a 3XX Response from an LRF  | 11.3.0 | 11.4.0 | C1-122499 |
| 2012-09        | CP-57 | CP-120583 | 4039 | 5   | SMS domain selection   | 11.4.0 | 11.5.0 | C1-123296 |
| 2012-09        | CP-57 | CP-120566 | 4068 | 5   | Emergency sub-service type handling  | 11.4.0 | 11.5.0 | C1-123416 |
| 2012-09        | CP-57 | CP-120597 | 4078 | 1   | Support of MRB Query mode in 3GPP TS 24.229  | 11.4.0 | 11.5.0 | C1-122938 |
| 2012-09        | CP-57 | CP-120603 | 4082 | 2   | Application servers and RAVEL  | 11.4.0 | 11.5.0 | C1-123288 |
| 2012-09        | CP-57 | CP-120586 | 4083 | 1   | Annex A updates for USSI   | 11.4.0 | 11.5.0 | C1-123264 |
| 2012-09        | CP-57 | CP-120588 | 4084 | 1   | Correction of correction to profile tables for use of 3GPP IM CN subsystem XML body in restoration procedures                        | 11.4.0 | 11.5.0 | C1-123172 |
| 2012-09        | CP-57 | CP-120588 | 4085 | 1   | Correcting profile tables for use of 3GPP IM CN subsystem XML body in response to request for emergency services                     | 11.4.0 | 11.5.0 | C1-123168 |
| 2012-09        | CP-57 | CP-120582 | 4088 | 2   | Reference update and technical changes: draft-ietf-sipcore-proxy-feature   | 11.4.0 | 11.5.0 | C1-123348 |
| 2012-09        | CP-57 | CP-120601 | 4089 | 1   | Annex A: P-Access-Network-Info in ACK  | 11.4.0 | 11.5.0 | C1-123256 |
| 2012-09        | CP-57 | CP-120569 | 4094 | 1   | Correction of SDP Profile about RFC 4145   | 11.4.0 | 11.5.0 | C1-123104 |
| 2012-09        | CP-57 | CP-120582 | 4097 | 1   | Feature-Caps header field part of trust domain   | 11.4.0 | 11.5.0 | C1-123158 |
| 2012-09        | CP-57 | CP-120599 | 4098 |     | Removing an EN regarding missing charging related headers  | 11.4.0 | 11.5.0 | C1-122680 |
| 2012-09        | CP-57 | CP-120603 | 4099 |     | Removing an EN regarding preservation of parameters in AS  | 11.4.0 | 11.5.0 | C1-122686 |
| 2012-09        | CP-57 | CP-120603 | 4100 |     | Removing EN regarding number normalization and enum translation  | 11.4.0 | 11.5.0 | C1-122687 |
| 2012-09        | CP-57 | CP-120603 | 4107 | 1   | IOI usage between TRF and terminating side   | 11.4.0 | 11.5.0 | C1-123284 |

| Change history |       |           |      |     |   |        |        |           |
|----------------|-------|-----------|------|-----|---|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old    | New    | WG doc    |
| 2012-09        | CP-57 | CP-120603 | 4108 | 1   | Co-location of TRF  | 11.4.0 | 11.5.0 | C1-123285 |
| 2012-09        | CP-57 | CP-120569 | 4114 | 1   | Correct handling of PPR in S-CSCF   | 11.4.0 | 11.5.0 | C1-123109 |
| 2012-09        | CP-57 | CP-120583 | 4115 | 1   | Correction ue initiated deregistration  | 11.4.0 | 11.5.0 | C1-123295 |
| 2012-09        | CP-57 | CP-120577 | 4118 | 1   | Condition for usage of Session-ID header filed within MESSAGE response            | 11.4.0 | 11.5.0 | C1-123134 |
| 2012-09        | CP-57 | CP-120597 | 4119 |     | Reference update: draft-ietf-mediactrl-mrb  | 11.4.0 | 11.5.0 | C1-122765 |
| 2012-09        | CP-57 | CP-120597 | 4120 | 3   | Visited network MRB information   | 11.4.0 | 11.5.0 | C1-123396 |
| 2012-09        | CP-57 | CP-120583 | 4121 | 3   | PCSCF discovery clarification   | 11.4.0 | 11.5.0 | C1-123440 |
| 2012-09        | CP-57 | CP-120600 | 4122 | 2   | Clarifications of used identities for registration procedures                     | 11.4.0 | 11.5.0 | C1-123355 |
| 2012-09        | CP-57 | CP-120588 | 4123 | 3   | DVB-RCS2 satellite access network as IP-CAN for IMS                               | 11.4.0 | 11.5.0 | C1-123428 |
| 2012-09        | CP-57 | CP-120600 | 4124 | 3   | Add reg-event changes for RFC 6140  | 11.4.0 | 11.5.0 | C1-123378 |
| 2012-09        | CP-57 | CP-120583 | 4126 | 1   | P-CSCF registration context lost  | 11.4.0 | 11.5.0 | C1-123297 |
| 2012-09        | CP-57 | CP-120588 | 4131 | 1   | Correction DHCP mechanism for P-CSCF discovery in Annex M                         | 11.4.0 | 11.5.0 | C1-123293 |
| 2012-09        | CP-57 | CP-120588 | 4132 | 1   | Correction to DHCP mechanism for P-CSCF discovery in Annex O                      | 11.4.0 | 11.5.0 | C1-123294 |
| 2012-09        | CP-57 | CP-120588 | 4133 |     | Correction to Annex 9.2   | 11.4.0 | 11.5.0 | C1-122849 |
| 2012-09        | CP-57 | CP-120570 | 4137 | 1   | Reference update: draft-ietf-mmusic-ice-tcp                                       | 11.4.0 | 11.5.0 | C1-123130 |
| 2012-09        | CP-57 | CP-120601 | 4140 | 1   | Network provided location information inserted by the MSC server enhanced for ICS | 11.4.0 | 11.5.0 | C1-123259 |
| 2012-09        | CP-57 | CP-120591 | 4146 |     | Specification of ISC gateway function – general clauses                           | 11.4.0 | 11.5.0 | C1-122928 |
| 2012-09        | CP-57 | CP-120591 | 4147 | 1   | Specification of ISC gateway function – SIP procedures                            | 11.4.0 | 11.5.0 | C1-123271 |
| 2012-09        | CP-57 | CP-120591 | 4148 | 1   | Specification of application gateway function – SDP procedures                    | 11.4.0 | 11.5.0 | C1-123272 |
| 2012-09        | CP-57 | CP-120588 | 4151 |     | Reversal of terminology change in annex D   | 11.4.0 | 11.5.0 | C1-122939 |
| 2012-09        | CP-57 | CP-120588 | 4152 | 1   | Emergency priority using the Resource-Priority header field                       | 11.4.0 | 11.5.0 | C1-123173 |
| 2012-09        | CP-57 | CP-120641 | 4153 | 3   | Description of overload control   | 11.4.0 | 11.5.0 | -         |
| 2012-09        | CP-57 | CP-120642 | 4154 | 3   | Support of overload control   | 11.4.0 | 11.5.0 | -         |
| 2012-09        | CP-57 | CP-120664 | 4156 | 5   | Media plane security  | 11.4.0 | 11.5.0 | -         |
| 2012-09        | CP-57 | CP-120576 | 4159 | 1   | mediasec ref deletions  | 11.4.0 | 11.5.0 | C1-123141 |
| 2012-09        | CP-57 | CP-120603 | 4162 |     | Updates to charging introduction for RAVEL  | 11.4.0 | 11.5.0 | C1-122968 |
| 2012-09        | CP-57 | CP-120588 | 4163 | 1   | Condition for restoration procedures causing UE reregistration                    | 11.4.0 | 11.5.0 | C1-123174 |
| 2012-09        | CP-57 | CP-120588 | 4164 | 1   | Missing procedure for NASS-IMS bundled authentication at S-CSCF                   | 11.4.0 | 11.5.0 | C1-123171 |
| 2012-09        | CP-57 | CP-120574 | 4180 | 2   | Emergency and normal registration independence                                    | 11.4.0 | 11.5.0 | C1-123374 |
| 2012-09        | CP-57 | CP-120606 | 4185 | 2   | Support of T.38 related SDP attributes  | 11.4.0 | 11.5.0 | C1-123400 |

| Change history |       |           |      |     |   |        |        |           |
|----------------|-------|-----------|------|-----|---|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old    | New    | WG doc    |
| 2012-09        | CP-57 | CP-120578 | 4188 |     | Correcting incorrect references in P-CSCF procedures when emergency call failure occurs | 11.4.0 | 11.5.0 | C1-123164 |
| 2012-09        | CP-57 | CP-120656 | 4189 | 1   | Reference list correction to align with the corrected TS 29.212 title                   | 11.4.0 | 11.5.0 | -         |
| 2012-12        | CP-58 | CP-120802 | 4106 | 5   | Additional guidance on use of 3xx responses   | 11.5.0 | 11.6.0 | C1-124983 |
| 2012-12        | CP-58 | CP-120802 | 4127 | 2   | Update the general requirements for tunnel procedures                                   | 11.5.0 | 11.6.0 | C1-123886 |
| 2012-12        | CP-58 | CP-120802 | 4128 | 4   | IP address obtained on S2a interface  | 11.5.0 | 11.6.0 | C1-124274 |
| 2012-12        | CP-58 | CP-120802 | 4129 | 4   | Tunnel modification by the UE   | 11.5.0 | 11.6.0 | C1-124275 |
| 2012-12        | CP-58 | CP-120802 | 4130 | 5   | Tunnel modification by the network  | 11.5.0 | 11.6.0 | C1-124276 |
| 2012-12        | CP-58 | CP-120804 | 4149 | 3   | Specification of ISC gateway function – SIP profile                                     | 11.5.0 | 11.6.0 | C1-124261 |
| 2012-12        | CP-58 | CP-120804 | 4150 | 2   | Specification of application gateway function – SDP profile                             | 11.5.0 | 11.6.0 | C1-124100 |
| 2012-12        | CP-58 | CP-120787 | 4187 | 1   | IANA registration of OMR parameters   | 11.5.0 | 11.6.0 | C1-123575 |
| 2012-12        | CP-58 | CP-120783 | 4196 |     | Delete IETF mediasec draft reference  | 11.5.0 | 11.6.0 | C1-123520 |
| 2012-12        | CP-58 | CP-120783 | 4197 |     | IMS media security profile table cleanup  | 11.5.0 | 11.6.0 | C1-123521 |
| 2012-12        | CP-58 | CP-120793 | 4201 | 4   | Contents of From and To header fields in SUBSCRIBE message                              | 11.5.0 | 11.6.0 | C1-124950 |
| 2012-12        | CP-58 | CP-120802 | 4202 | 4   | Correction on handling of rn parameter and npdi parameter at S-CSCF.                    | 11.5.0 | 11.6.0 | C1-125015 |
| 2012-12        | CP-58 | CP-120821 | 4203 | 2   | Support of T.38 SDP attributes in IMS   | 11.5.0 | 11.6.0 | C1-124158 |
| 2012-12        | CP-58 | CP-120801 | 4204 | 1   | Transit-ioi is removed from forwarded message to visited network                        | 11.5.0 | 11.6.0 | C1-124092 |
| 2012-12        | CP-58 | CP-120815 | 4205 | 5   | Overload control clarifications   | 11.5.0 | 11.6.0 | C1-125010 |
| 2012-12        | CP-58 | CP-120812 | 4206 | 3   | Removing ENs about IBCF and OMR   | 11.5.0 | 11.6.0 | C1-124262 |
| 2012-12        | CP-58 | CP-120812 | 4207 |     | Removing an EN regarding PSI  | 11.5.0 | 11.6.0 | C1-123620 |
| 2012-12        | CP-58 | CP-120812 | 4212 |     | Correcting the UE-originating case indication   | 11.5.0 | 11.6.0 | C1-123630 |
| 2012-12        | CP-58 | CP-120793 | 4214 | 6   | Correcting procedures for re-establishment a context for SIP signalling                 | 11.5.0 | 11.6.0 | C1-124952 |
| 2012-12        | CP-58 | CP-120773 | 4219 | 4   | Correction of emergency sub-service type handling                                       | 11.5.0 | 11.6.0 | C1-124284 |
| 2012-12        | CP-58 | CP-120793 | 4220 | 2   | Remaining corrections to emergency sub-service type handling                            | 11.5.0 | 11.6.0 | C1-124181 |
| 2012-12        | CP-58 | CP-120782 | 4223 | 2   | Corrections to E-CSCF and LRF handling for emergency calls                              | 11.5.0 | 11.6.0 | C1-124764 |
| 2012-12        | CP-58 | CP-120812 | 4224 |     | Application servers and RAVEL   | 11.5.0 | 11.6.0 | C1-123577 |
| 2012-12        | CP-58 | CP-120777 | 4228 | 1   | Correction of 3GPP IM CN subsystem XML handling   | 11.5.0 | 11.6.0 | C1-123972 |
| 2012-12        | CP-58 | CP-120793 | 4229 | 3   | PCSCF discovery Annex L editorial   | 11.5.0 | 11.6.0 | C1-124989 |
| 2012-12        | CP-58 | CP-120776 | 4234 |     | Table A.162, item 61 referencing incorrect document                                     | 11.5.0 | 11.6.0 | C1-123669 |
| 2012-12        | CP-58 | CP-120802 | 4235 | 1   | SDP impacts due to IP-CAN bearer release  | 11.5.0 | 11.6.0 | C1-124006 |
| 2012-12        | CP-58 | CP-120802 | 4236 | 1   | Precondition and INVITE without SDP offer   | 11.5.0 | 11.6.0 | C1-124007 |



| Change history |       |           |      |     |  |        |        |           |
|----------------|-------|-----------|------|-----|--|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old    | New    | WG doc    |
| 2012-12        | CP-58 | CP-120802 | 4237 | 1   | User rejecting media stream during set up of multimedia session    | 11.5.0 | 11.6.0 | C1-124008 |
| 2012-12        | CP-58 | CP-120812 | 4239 | 1   | Decision on loop back routing in S-CSCF                            | 11.5.0 | 11.6.0 | C1-124102 |
| 2012-12        | CP-58 | CP-120793 | 4241 | 1   | Correct Definition of Temporarily Authorized Resource-Priority     | 11.5.0 | 11.6.0 | C1-124003 |
| 2012-12        | CP-58 | CP-120791 | 4243 | 2   | Reference update: draft-ietf-sipcore-proxy-feature                 | 11.5.0 | 11.6.0 | C1-124766 |
| 2012-12        | CP-58 | CP-120791 | 4244 | 1   | Feature-Caps header field in target refresh requests and responses | 11.5.0 | 11.6.0 | C1-124122 |
| 2012-12        | CP-58 | CP-120804 | 4247 | 1   | Specification of application gateway function – SDP procedures     | 11.5.0 | 11.6.0 | C1-124098 |
| 2012-12        | CP-58 | CP-120810 | 4248 | 1   | Profiles change for P-Access-Network-Info header                   | 11.5.0 | 11.6.0 | C1-124111 |
| 2012-12        | CP-58 | CP-120810 | 4249 | 3   | Correction to the coding of UE-time-zone                           | 11.5.0 | 11.6.0 | C1-124273 |
| 2012-12        | CP-58 | CP-120810 | 4250 | 2   | Removal of Editor's Note on NPLI inserted by both P-CSCF and AS    | 11.5.0 | 11.6.0 | C1-124223 |
| 2012-12        | CP-58 | CP-120793 | 4251 | 1   | Correct emergency call description when roaming                    | 11.5.0 | 11.6.0 | C1-124116 |
| 2012-12        | CP-58 | CP-120782 | 4254 |     | Dialog state notification clarification                            | 11.5.0 | 11.6.0 | C1-123752 |
| 2012-12        | CP-58 | CP-120785 | 4257 | 1   | Emergency and normal registration independence                     | 11.5.0 | 11.6.0 | C1-123994 |
| 2012-12        | CP-58 | CP-120815 | 4258 | 5   | Overload control -Inconstancies correction                         | 11.5.0 | 11.6.0 | C1-125009 |
| 2012-12        | CP-58 | CP-120815 | 4262 | 3   | Event-based overload control procedures                            | 11.5.0 | 11.6.0 | C1-124856 |
| 2012-12        | CP-58 | CP-120780 | 4263 | 2   | Correction to integrity-protected usage in S-CSCF                  | 11.5.0 | 11.6.0 | C1-124150 |
| 2012-12        | CP-58 | CP-120809 | 4273 |     | Mz Reference Point – ISC alternative                               | 11.5.0 | 11.6.0 | C1-124301 |
| 2012-12        | CP-58 | CP-120812 | 4275 | 1   | Removing the g.3gpp.loopback in TRF                                | 11.5.0 | 11.6.0 | C1-124850 |
| 2012-12        | CP-58 | CP-120788 | 4281 |     | Reference update: RFC 6679   | 11.5.0 | 11.6.0 | C1-124369 |
| 2012-12        | CP-58 | CP-120775 | 4285 | 3   | Updating IMEI URN draft reference                                  | 11.5.0 | 11.6.0 | C1-125006 |
| 2012-12        | CP-58 | CP-120793 | 4286 | 2   | Default ICSI value selected by S-CSCF                              | 11.5.0 | 11.6.0 | C1-124951 |
| 2012-12        | CP-58 | CP-120810 | 4287 |     | Correction of "UE-time-zone" to "local-time-zone" in TS 24.229     | 11.5.0 | 11.6.0 | C1-124433 |
| 2012-12        | CP-58 | CP-120801 | 4288 |     | Transit IOI general description                                    | 11.5.0 | 11.6.0 | C1-124439 |
| 2012-12        | CP-58 | CP-120801 | 4289 | 1   | Including transit-IOI in SIP responses                             | 11.5.0 | 11.6.0 | C1-124843 |
| 2012-12        | CP-58 | CP-120802 | 4294 | 1   | Removal of internal references from IBCF procedures                | 11.5.0 | 11.6.0 | C1-124772 |
| 2012-12        | CP-58 | CP-120815 | 4296 | 2   | Closure of open issues in IOC work item                            | 11.5.0 | 11.6.0 | C1-125008 |
| 2012-12        | CP-58 | CP-120793 | 4299 | 1   | P-CSCF registration context lost – text correction                 | 11.5.0 | 11.6.0 | C1-124896 |
| 2012-12        | CP-58 | CP-120793 | 4300 |     | NAT detection by the UE- text correction                           | 11.5.0 | 11.6.0 | C1-124521 |
| 2012-12        | CP-58 | CP-120780 | 4305 |     | Correction on integrity-protected handling in S-CSCF               | 11.5.0 | 11.6.0 | C1-124528 |
| 2012-12        | CP-58 | CP-120793 | 4311 | 1   | Correction to challenge response examination in P-CSCF             | 11.5.0 | 11.6.0 | C1-124903 |
| 2013-03        | CP-59 | CP-130093 | 4139 | 6   | IBCF don't change the dialog-ID                                    | 11.6.0 | 11.7.0 | C1-130555 |
| 2013-03        | CP-59 | CP-130117 | 4238 | 3   | Network provided cell identity for UTRAN                           | 11.6.0 | 11.7.0 | C1-130501 |

| Change history |       |           |      |     |  |        |        |           |
|----------------|-------|-----------|------|-----|--|--------|--------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old    | New    | WG doc    |
| 2013-03        | CP-59 | CP-130110 | 4246 | 4   | Specification of ISC gateway function – SIP procedures   | 11.6.0 | 11.7.0 | C1-130336 |
| 2013-03        | CP-59 | CP-130117 | 4301 | 5   | Network provided Geographical Identifier   | 11.6.0 | 11.7.0 | C1-130915 |
| 2013-03        | CP-59 | CP-130099 | 4314 | 4   | Correct determination of the status of being available for voice over PS                                     | 11.6.0 | 11.7.0 | C1-130892 |
| 2013-03        | CP-59 | CP-130116 | 4315 | 3   | Correcting availability for calls when dedicated bearer suitable for SIP signalling is used                  | 11.6.0 | 11.7.0 | C1-130897 |
| 2013-03        | CP-59 | CP-130117 | 4324 | 1   | P-CSCF handling of PANI in case PCRF is used   | 11.6.0 | 11.7.0 | C1-130502 |
| 2013-03        | CP-59 | CP-130098 | 4327 | 1   | Security Client header in case of Media Sec  | 11.6.0 | 11.7.0 | C1-130536 |
| 2013-03        | CP-59 | CP-130107 | 4331 | 1   | Support for P-Charging-Vector in SIP ACK   | 11.6.0 | 11.7.0 | C1-130512 |
| 2013-03        | CP-59 | CP-130107 | 4332 | 1   | Replacement of RFC3455 by draft-drage-sipping-rfc3455bis-06  | 11.6.0 | 11.7.0 | C1-130564 |
| 2013-03        | CP-59 | CP-130107 | 4333 | 1   | Clarification of handling IOI parameter at S-CSCF  | 11.6.0 | 11.7.0 | C1-130565 |
| 2013-03        | CP-59 | CP-130107 | 4334 | 3   | Clarification of handling IOI parameters at transit function   | 11.6.0 | 11.7.0 | C1-130895 |
| 2013-03        | CP-59 | CP-130102 | 4337 |     | Reference update: RFC 6809   | 11.6.0 | 11.7.0 | C1-130143 |
| 2013-03        | CP-59 | CP-130116 | 4440 |     | Correcting reference to PSU extension  | 11.6.0 | 11.7.0 | C1-130164 |
| 2013-03        | CP-59 | CP-130116 | 4441 | 1   | ICSI in Contact and Accept-Contact header fields   | 11.6.0 | 11.7.0 | C1-130746 |
| 2013-03        | CP-59 | CP-130101 | 4447 | 2   | Annex A updates for RFC5506  | 11.6.0 | 11.7.0 | C1-130797 |
| 2013-03        | CP-59 | CP-130101 | 4450 | 2   | Annex A updates for RFC3611  | 11.6.0 | 11.7.0 | C1-130814 |
| 2013-03        | CP-59 | CP-130116 | 4451 | 2   | Annex A updates for 3gpp_MaxRecvSDUSize SDP attributes   | 11.6.0 | 11.7.0 | C1-130827 |
| 2013-03        | CP-59 | CP-130094 | 4462 | 1   | Correction of subclause reference in dialstring related procedures   | 11.6.0 | 11.7.0 | C1-130739 |
| 2013-03        | CP-59 | CP-130098 | 4469 |     | Delete IETF mediasec draft reference   | 11.6.0 | 11.7.0 | C1-130328 |
| 2013-03        | CP-59 | CP-130101 | 4471 |     | Correction of references to annex G and annex F  | 11.6.0 | 11.7.0 | C1-130334 |
| 2013-03        | CP-59 | CP-130121 | 4472 |     | Interaction between overload control mechanisms  | 11.6.0 | 11.7.0 | C1-130337 |
| 2013-03        | CP-59 | CP-130098 | 4480 | 1   | IANA registration issues for a=3ge2ae  | 11.6.0 | 11.7.0 | C1-130539 |
| 2013-03        | CP-59 | CP-130096 | 4483 | 1   | Profile changes relating to CRS  | 11.6.0 | 11.7.0 | C1-130542 |
| 2013-06        | CP-60 | CP-130233 | 4145 | 8   | Removal of dialled digits option from emergency call generation  | 11.7.0 | 11.8.0 | C1-132563 |
| 2013-06        | CP-60 | CP-130231 | 4446 | 4   | UE indicating type of emergency service when 380 response is received  | 11.7.0 | 11.8.0 | C1-131923 |
| 2013-06        | CP-60 | CP-130227 | 4455 | 4   | Not reachable for SIP signalling due to unclear requirement on re-establishment of the SIP signalling bearer | 11.7.0 | 11.8.0 | C1-131409 |
| 2013-06        | CP-60 | CP-130230 | 4475 | 4   | Emergency bearer support and IMS Emergency correction  | 11.7.0 | 11.8.0 | C1-131413 |
| 2013-06        | CP-60 | CP-130222 | 4498 | 3   | Updating MMUSIC draft references for ICS User Agent and SCC Application Server                               | 11.7.0 | 11.8.0 | C1-132291 |
| 2013-06        | CP-60 | CP-130240 | 4501 | 1   | Reference update of draft-atarius-dispatch-meid-urn  | 11.7.0 | 11.8.0 | C1-131542 |
| 2013-06        | CP-60 | CP-130252 | 4515 |     | Syntax for "local-time-zone" incorrect   | 11.7.0 | 11.8.0 | C1-131083 |
| 2013-06        | CP-60 | CP-130242 | 4528 | 1   | "transit-ioi" header field parameter correction  | 11.7.0 | 11.8.0 | C1-131632 |

| Change history |       |           |      |     |   |        |         |           |
|----------------|-------|-----------|------|-----|---|--------|---------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old    | New     | WG doc    |
| 2013-06        | CP-60 | CP-130253 | 4530 |     | Removing RAVEL EN related to charging indicators  | 11.7.0 | 11.8.0  | C1-131150 |
| 2013-06        | CP-60 | CP-130253 | 4532 | 1   | IOI exchange when loopback routeing occurs  | 11.7.0 | 11.8.0  | C1-131620 |
| 2013-06        | CP-60 | CP-130253 | 4534 | 1   | Handling of transit IOI when loopback routeing occurs   | 11.7.0 | 11.8.0  | C1-131622 |
| 2013-06        | CP-60 | CP-130251 | 4570 | 1   | Removal of Editor's Note on maximum number of registration flows  | 11.7.0 | 11.8.0  | C1-131634 |
| 2013-06        | CP-60 | CP-130220 | 4584 | 3   | Prevent receipt of normal call at the UE while it is attached for emergency services only   | 11.7.0 | 11.8.0  | C1-132626 |
| 2013-06        | CP-60 | CP-130225 | 4608 | 2   | Consolidation of DTMF info package definition in 3GPP TS 24.229   | 11.7.0 | 11.8.0  | C1-132579 |
| 2013-09        | CP-61 | CP-130481 | 4615 | 1   | Updating IMEI URN draft reference   | 11.8.0 | 11.9.0  | C1-133251 |
| 2013-09        | CP-61 | CP-130493 | 4628 |     | Via header field handling on Privacy protection at IBCF   | 11.8.0 | 11.9.0  | C1-132755 |
| 2013-09        | CP-61 | CP-130483 | 4633 | 1   | Reference update of draft-vanelburg-dispatch-private-network-ind  | 11.8.0 | 11.9.0  | C1-133264 |
| 2013-09        | CP-61 | CP-130501 | 4647 | 3   | Identifying the home network to TRF   | 11.8.0 | 11.9.0  | C1-133610 |
| 2013-09        | CP-61 | CP-130500 | 4651 | 1   | IMS debug removal of feature  | 11.8.0 | 11.9.0  | C1-133311 |
| 2013-09        | CP-61 | CP-130488 | 4665 | 1   | Fixing essential issues in RTP media security   | 11.8.0 | 11.9.0  | C1-133504 |
| 2013-12        | CP-62 | CP-130726 | 4672 |     | Reverting subclause heading voided in error   | 11.9.0 | 11.10.0 | C1-133675 |
| 2013-12        | CP-62 | CP-130722 | 4676 | 1   | Reference update of draft-vanelburg-dispatch-private-network-ind  | 11.9.0 | 11.10.0 | C1-134199 |
| 2013-12        | CP-62 | CP-130728 | 4680 |     | Reference update: draft-kaplan-insipid-session-id   | 11.9.0 | 11.10.0 | C1-133694 |
| 2013-12        | CP-62 | CP-130748 | 4682 | 1   | Reference update: draft-ietf-soc-overload-control, draft-ietf-soc-overload-rate-control and draft-ietf-soc-load-control-event-package | 11.9.0 | 11.10.0 | C1-134438 |
| 2013-12        | CP-62 | CP-130743 | 4684 | 1   | Reference update: RFC 6917 (draft-ietf-mediactrl-mrb)   | 11.9.0 | 11.10.0 | C1-134188 |
| 2013-12        | CP-62 | CP-130721 | 4691 | 1   | Reference update: RFC 7006 (draft-ietf-mmusic-sdp-miscellaneous-caps)   | 11.9.0 | 11.10.0 | C1-134209 |
| 2013-12        | CP-62 | CP-130733 | 4715 | 3   | Use of ECN in Multimedia Priority Service   | 11.9.0 | 11.10.0 | C1-134373 |
| 2013-12        | CP-62 | CP-130729 | 4721 |     | Fixing remaining errors in media security   | 11.9.0 | 11.10.0 | C1-133920 |
| 2013-12        | CP-62 | CP-130731 | 4729 | 4   | Correction when receiving a 380 (Alternative Service) response indicating "emergency" to UE non-detectable IMS emergency call         | 11.9.0 | 11.10.0 | C1-134905 |
| 2013-12        | CP-62 | CP-130720 | 4740 |     | Reference Update: draft-ietf-salud-alert-info-urns  | 11.9.0 | 11.10.0 | CP-130720 |
| 2013-12        | CP-62 | CP-130744 | 4750 |     | Correct Annex A due to 3xx response containing a Contact header field   | 11.9.0 | 11.10.0 | C1-134570 |
| 2013-12        | CP-62 | CP-130746 | 4755 |     | utran-sai-id-3gpp and utran-sai-3gpp  | 11.9.0 | 11.10.0 | C1-134609 |
| 2013-12        | CP-62 | CP-130747 | 4761 | 1   | Home network bypassing of E.164 translation   | 11.9.0 | 11.10.0 | C1-135007 |
| 2013-12        | CP-62 | CP-130721 | 4766 | 1   | Updating IMEI URN draft reference   | 11.9.0 | 11.10.0 | C1-134987 |
| 2013-12        | CP-62 | CP-130736 | 4782 |     | Incorrect preconditions for inclusion of P-Refused-URI-List and Retry-After header fields in INVITE                                   | 11.9.0 | 11.10.0 | C1-135118 |

| Change history |       |           |      |     |   |         |         |           |
|----------------|-------|-----------|------|-----|---|---------|---------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment   | Old     | New     | WG doc    |
| 2014-03        | CP-63 | CP-140126 | 4784 | 2   | Clarify that SDP for sessions with voice media can be updated in a TA indicating voice over PS is not supported             | 11.10.0 | 11.11.0 | C1-140400 |
| 2014-03        | CP-63 | CP-140133 | 4788 |     | Re-adding 3gpp body xml schema to archive   | 11.10.0 | 11.11.0 | C1-140031 |
| 2014-03        | CP-63 | CP-140128 | 4790 | 2   | Correction on syntax of values of feature capability indicators   | 11.10.0 | 11.11.0 | C1-140660 |
| 2014-03        | CP-63 | CP-140115 | 4795 |     | Reference update of draft-vanelburg-dispatch-private-network-ind  | 11.10.0 | 11.11.0 | C1-140051 |
| 2014-03        | CP-63 | CP-140115 | 4801 | 1   | Correcting P-Private-Network-Indication descriptions in response  | 11.10.0 | 11.11.0 | C1-140470 |
| 2014-03        | CP-63 | CP-140121 | 4808 | 3   | Non UE detected emergency call correction for retry in CS domain  | 11.10.0 | 11.11.0 | C1-140777 |
| 2014-03        | CP-63 | CP-140134 | 4811 | 1   | Removing of the left IMS debug feature parts  | 11.10.0 | 11.11.0 | C1-140486 |
| 2014-03        | CP-63 | CP-140119 | 4814 | 1   | Lost procedures for handling Retry-After in failure response to REGISTER request  | 11.10.0 | 11.11.0 | C1-140477 |
| 2014-03        | CP-63 | CP-140128 | 4817 |     | Correcting g.3gpp.home visited feature-capability indicator name  | 11.10.0 | 11.11.0 | C1-140189 |
| 2014-03        | CP-63 | CP-140114 | 4822 | 1   | Updating IMEI URN draft reference   | 11.10.0 | 11.11.0 | C1-140499 |
| 2014-03        | CP-63 | CP-140113 | 4829 | 2   | Allocating a GRUU when the explicitly registered IMPU is barred   | 11.10.0 | 11.11.0 | C1-140692 |
| 2014-03        | CP-63 | CP-140113 | 4851 | 1   | Generation of Public GRUU   | 11.10.0 | 11.11.0 | C1-140698 |
| 2014-06        | CP-64 | CP-140296 | 4864 | 3   | Corrections for voice centric UE to continue being reachable for IMS voice when P-CSCF serving the UE stops being available | 11.11.0 | 11.12.0 | C1-141554 |
| 2014-06        | CP-64 | CP-140302 | 4870 | 1   | IOI exchange between the SCC AS and ATCF  | 11.11.0 | 11.12.0 | C1-141499 |
| 2014-06        | CP-64 | CP-140295 | 4893 | 1   | Reference update of draft-vanelburg-dispatch-private-network-ind  | 11.11.0 | 11.12.0 | C1-141805 |
| 2014-06        | CP-64 | CP-140291 | 4907 |     | Syntax for OLI is incorrect   | 11.11.0 | 11.12.0 | C1-141034 |
| 2014-06        | CP-64 | CP-140294 | 4912 | 1   | GRUU validation   | 11.11.0 | 11.12.0 | C1-141366 |
| 2014-06        | CP-64 | CP-140296 | 4918 | 2   | Clarification of payload type usage for telephony-events  | 11.11.0 | 11.12.0 | C1-141628 |
| 2014-06        | CP-64 | CP-140300 | 4921 |     | Profile table changes for SDES media plane security role  | 11.11.0 | 11.12.0 | C1-141056 |
| 2014-06        | CP-64 | CP-140307 | 4939 | 1   | EN removal: Feature-capability indicator IANA registration status   | 11.11.0 | 11.12.0 | C1-142255 |
| 2014-06        | CP-64 | CP-140311 | 4941 | 1   | Correction of g.3gpp.icsi-ref feature-capability indicator definition   | 11.11.0 | 11.12.0 | C1-142257 |
| 2014-06        | CP-64 | CP-140299 | 4960 | 2   | Solution for editor's note related to draft-ietf-sipcore-rfc4244bis-00  | 11.11.0 | 11.12.0 | C1-142450 |
| 2014-06        | CP-64 | CP-140292 | 4966 | 2   | URI matching for terminating requests   | 11.11.0 | 11.12.0 | C1-142440 |
| 2014-06        | CP-64 | CP-140294 | 4974 | 1   | Updating CS-SDP draft reference to RFC 7195   | 11.11.0 | 11.12.0 | C1-142240 |
| 2014-06        | CP-64 | CP-140304 | 4981 | 1   | Update draft-atarius-dispatch-meid-urn  | 11.11.0 | 11.12.0 | C1-142253 |
| 2014-06        | CP-64 | CP-140305 | 4991 | 1   | Reference update for overload control   | 11.11.0 | 11.12.0 | C1-142262 |
| 2014-06        | CP-64 | CP-140306 | 5001 |     | EN removal: Feature-capability indicator IANA registration status, MRB  | 11.11.0 | 11.12.0 | C1-142475 |

| Change history |       |           |      |     |  |         |         |           |
|----------------|-------|-----------|------|-----|--|---------|---------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old     | New     | WG doc    |
| 2014-09        | CP-65 | CP-140634 | 4948 | 3   | Resolving interoperability problems caused by insufficiently documented UE precondition handling - alternative A                     | 11.12.0 | 11.13.0 | C1-143295 |
| 2014-09        | CP-65 | CP-140633 | 5011 | 1   | Updating IMEI URN draft reference to RFC 7254  | 11.12.0 | 11.13.0 | C1-143084 |
| 2014-09        | CP-65 | CP-140644 | 5014 |     | EN removal: g.3gpp.icsi-ref feature-capability indicator IANA registration status  | 11.12.0 | 11.13.0 | C1-142590 |
| 2014-09        | CP-65 | CP-140641 | 5024 | 1   | ICE in IBCF  | 11.12.0 | 11.13.0 | C1-143101 |
| 2014-12        | CP-66 | CP-140823 | 5056 | 1   | Reference Update: RFC7315  | 11.13.0 | 11.14.0 | C1-143982 |
| 2014-12        | CP-66 | CP-140818 | 5060 | 1   | Reference update: RFC 7329 (draft-kaplan-insipid-session-id)   | 11.13.0 | 11.14.0 | C1-143969 |
| 2014-12        | CP-66 | CP-140816 | 5073 | 1   | Reference update from draft-vanelburg-dispatch-private-network-ind to RFC 7316   | 11.13.0 | 11.14.0 | C1-143964 |
| 2014-12        | CP-66 | CP-140826 | 5077 | 2   | Editor's note on ICSI usage  | 11.13.0 | 11.14.0 | C1-144771 |
| 2014-12        | CP-66 | CP-140826 | 5103 | 1   | EN combination of emergency call types   | 11.13.0 | 11.14.0 | C1-143992 |
| 2014-12        | CP-66 | CP-140828 | 5127 |     | Reference update: SIP overload control   | 11.13.0 | 11.14.0 | C1-144303 |
| 2015-03        | CP-67 | CP-150050 | 5182 |     | Reference update for UUSIW   | 11.14.0 | 11.15.0 | C1-150108 |
| 2015-03        | CP-67 | CP-150053 | 5193 |     | Reference update: RFC 7135 (was draft-polk-local-emergency-rph-namespace)  | 11.14.0 | 11.15.0 | C1-150124 |
| 2015-03        | CP-67 | CP-150044 | 5213 | 2   | Correction of P-Charging-Vector access-network-charging-info syntax – Alt 2  | 11.14.0 | 11.15.0 | C1-150694 |
| 2015-03        | CP-67 | CP-150044 | 5219 | 1   | Handling of P-Charging-Function-Addresses  | 11.14.0 | 11.15.0 | C1-150538 |
| 2015-06        | CP-68 | CP-150287 | 5268 | 1   | Reference Update: RFC7462 (alert-info urns)  | 11.15.0 | 11.16.0 | C1-151398 |
| 2015-06        | CP-68 | CP-150299 | 5271 | 1   | Delete Debug Leftovers   | 11.15.0 | 11.16.0 | C1-151440 |
| 2015-06        | CP-68 | CP-150297 | 5274 | 1   | Clarifying condition for not routing via S-CSCF for an emergency call  | 11.15.0 | 11.16.0 | C1-151437 |
| 2015-06        | CP-68 | CP-150293 | 5288 | 1   | Corrections to media plane security  | 11.15.0 | 11.16.0 | C1-151426 |
| 2015-06        | CP-68 | CP-150289 | 5311 | 1   | Removing THIG on Path and Service-Route header fields  | 11.15.0 | 11.16.0 | C1-151417 |
| 2015-06        | CP-68 | CP-150294 | 5319 | 3   | Update 3GPP2 reference to reflect the correct published version  | 11.15.0 | 11.16.0 | C1-151601 |
| 2015-06        | CP-68 | CP-150300 | 5327 | 4   | Translation of geo-local numbers   | 11.15.0 | 11.16.0 | C1-152209 |
| 2015-06        | CP-68 | CP-150300 | 5332 | 3   | Loopback indication in responses   | 11.15.0 | 11.16.0 | C1-152261 |
| 2015-06        | CP-68 | CP-150292 | 5342 | 1   | Modification of missing Allow-Events header field status in annex A  | 11.15.0 | 11.16.0 | C1-152170 |
| 2015-06        | CP-68 | CP-150289 | 5377 | 1   | Content-Disposition for pdf+xml message bodies   | 11.15.0 | 11.16.0 | C1-152159 |
| 2015-09        | CP-69 | CP-150504 | 5411 |     | Reference update: RFC 7415   | 11.16.0 | 11.17.0 | C1-152658 |
| 2015-12        | CP-70 | CP-150680 | 5483 | 1   | P-Access-Network-Info ABNF Update  | 11.17.0 | 11.18.0 | C1-154562 |
| 2015-12        | CP-70 | CP-150681 | 5504 | 1   | Adding the loopback-indication in subsequent requests  | 11.17.0 | 11.18.0 | C1-154568 |
| 2015-12        | CP-70 | CP-150681 | 5509 | 1   | Loopback indication in Responses   | 11.17.0 | 11.18.0 | C1-154565 |
| 2015-12        | CP-70 | CP-150677 | 5520 |     | Call modification: UE shall not indicate the requirement for the precondition mechanism by using the Require header field mechanism. | 11.17.0 | 11.18.0 | C1-154232 |

| Change history |       |           |      |     |  |         |         |           |
|----------------|-------|-----------|------|-----|--|---------|---------|-----------|
| Date           | TSG # | TSG Doc.  | CR   | Rev | Subject/Comment  | Old     | New     | WG doc    |
| 2016-03        | CP-71 | CP-160065 | 5534 | 1   | Reference correction in Table A.3A   | 11.18.0 | 11.19.0 | C1-160440 |
| 2016-03        | CP-71 | CP-160066 | 5540 |     | Correction of the incorrect referenced subclause number.                                   | 11.18.0 | 11.19.0 | C1-160153 |
| 2016-03        | CP-71 | CP-160064 | 5546 | 2   | MGCF call initiation: removing possibility for using require header field in preconditions | 11.18.0 | 11.19.0 | C1-160485 |
| 2016-06        | CP-72 | CP-160298 | 5582 | 1   | orig-cdiv session case definition from draft-mohali-dispatch-originating-cdiv-parameter-01 | 11.19.0 | 11.20.0 | C1-162091 |
| 2016-06        | CP-72 | CP-160298 | 5586 |     | Correction of the incorrect referenced subclause number                                    | 11.19.0 | 11.20.0 | C1-161634 |
| 2016-06        | CP-72 | CP-160297 | 5589 | 1   | aSRVCC not working when terminating UE does not send 183 response                          | 11.19.0 | 11.20.0 | C1-162089 |
| 2016-06        | CP-72 | CP-160298 | 5594 | 2   | Updates to RFC 7315 P-header extensions usage in SIP requests/responses                    | 11.19.0 | 11.20.0 | C1-162469 |
| 2016-06        | CP-72 | CP-160298 | 5624 | 1   | Reference update: draft-holmberg-dispatch-pani-abnf  | 11.19.0 | 11.20.0 | C1-162862 |

| Change history |         |           |      |     |     |  |             |  |
|----------------|---------|-----------|------|-----|-----|--|-------------|--|
| Date           | Meeting | TDoc      | CR   | Rev | Cat | Subject/Comment  | New version |  |
| 2016-09        | CT#73   | CP-160483 | 5659 | 1   | A   | P-CSCF includes access-network-charging-info in reliable response    | 11.21.0     |  |
| 2016-09        | CT#73   | CP-160483 | 5682 | 1   | A   | Correction on support of P-Asserted-Identity header                  | 11.21.0     |  |
| 2016-09        | CT#73   | CP-160484 | 5693 |     | F   | Reference update: RFC 7913   | 11.21.0     |  |
| 2016-12        | CT#74   | CP-160708 | 5698 | 2   | A   | Correction on support of P-Asserted-Service header                   | 11.22.0     |  |
| 2016-12        | CT#74   | CP-160711 | 5721 |     | F   | Updated ref to draft-mohali-dispatch-originating-cdiv-parameter-02   | 11.22.0     |  |
| 2016-12        | CT#74   | CP-160711 | 5727 |     | F   | Reference update: RFC 7976   | 11.22.0     |  |
| 2016-12        | CT#74   | CP-160710 | 5759 | 2   | A   | IPv4 and IPv6 support in UE  | 11.22.0     |  |
| 2017-03        | CT#75   | CP-170105 | 5795 |     | F   | Updated ref to draft-mohali-dispatch-originating-cdiv-parameter-03   | 11.23.0     |  |
| 2017-03        | CT#75   | CP-170103 | 5825 | 1   | A   | Update IANA registration template for infoDtmf                       | 11.23.0     |  |
| 2017-03        | CT#75   | CP-170104 | 5831 |     | A   | IANA registration for e2ae complete                                  | 11.23.0     |  |
| 2017-06        | CT#76   | CP-171056 | 5892 | 1   | F   | Updated reference to draft-mohali-sipcore-originating-cdiv-parameter | 11.24.0     |  |
| 2017-06        | CT#76   | CP-171054 | 5936 |     | A   | Update draft-atarius-dispatch-meid-urn reference                     | 11.24.0     |  |
| 2017-09        | CT#77   | CP-172084 | 5949 |     |     | IANA registratin for DTMF info package complete                      | 11.25.0     |  |
| 2017-12        | CT#78   | CP-173046 | 5988 | 1   | F   | Update draft ref for Originating-CDIV param in P-Served-User         | 11.26.0     |  |
| 2018-09        | CT#81   | CP-182113 | 6151 | 1   | F   | Update draft ref for Originating-CDIV param in P-Served-User         | 11.27.0     |  |
| 2018-12        | CT#82   | CP-183072 | 6189 | 1   | A   | Change reference from IETF draft to RFC                              | 11.28.0     |  |
| 2018-12        | CT#82   | CP-183051 | 6201 | 1   | A   | Determining the originating network of the I-WLAN AP                 | 11.28.0     |  |
| 2018-12        | CT#82   | CP-183052 | 6208 | 2   | F   | Update draft ref for Originating-CDIV param in P-Served-User         | 11.28.0     |  |
| 2018-12        | CT#82   | CP-183052 | 6236 | 1   | F   | Delete EN in R.3.2.1   | 11.28.0     |  |

## History

| <b>Document history</b> |               |             |
|-------------------------|---------------|-------------|
| V11.5.0                 | November 2012 | Publication |
| V11.6.0                 | January 2013  | Publication |
| V11.7.0                 | April 2013    | Publication |
| V11.8.0                 | July 2013     | Publication |
| V11.9.0                 | October 2013  | Publication |
| V11.10.0                | January 2014  | Publication |
| V11.11.0                | April 2014    | Publication |
| V11.12.0                | July 2014     | Publication |
| V11.13.0                | October 2014  | Publication |
| V11.14.0                | February 2015 | Publication |
| V11.15.0                | April 2015    | Publication |
| V11.16.0                | July 2015     | Publication |
| V11.17.0                | October 2015  | Publication |
| V11.18.0                | January 2016  | Publication |
| V11.19.0                | May 2016      | Publication |
| V11.20.0                | July 2016     | Publication |
| V11.21.0                | October 2016  | Publication |
| V11.22.0                | January 2017  | Publication |
| V11.23.0                | March 2017    | Publication |
| V11.24.0                | July 2017     | Publication |
| V11.25.0                | October 2017  | Publication |
| V11.26.0                | January 2018  | Publication |
| V11.27.0                | November 2018 | Publication |
| V11.28.0                | January 2019  | Publication |