ETSITS 124 229 V5.26.0 (2012-03)



Digital cellular telecommunications system (Phase 2+); 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 5.26.0 Release 5)



Reference RTS/TSGC-0124229v5q0 Keywords GSM,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

Individual copies of the present document can be downloaded from: http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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

http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services: http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2012. All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP**TM and **LTE**TM are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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 (http://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.

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.

Contents

Intelle	ntellectual Property Rights2			
Forew	ord	2		
Forew	vord	9		
1	Scope	10		
2	References	10		
3	Definitions and abbreviations	13		
3.1	Definitions	13		
3.2	Abbreviations			
4	General	16		
4.1	Conformance of IM CN subsystem entities to SIP, SDP and other protocols	16		
4.2	URI and address assignments			
4.2A	Transport mechanisms			
4.3	Routeing principles of IM CN subsystem entities			
4.4	Trust domain			
4.5	Charging correlation principles for IM CN subsystems			
4.5.1	Overview			
4.5.2	IM CN subsystem charging identifier (ICID)	19		
4.5.3	Access network charging information			
4.5.3.1	General	19		
4.5.3.2	GPRS charging information	19		
4.5.4	Inter operator identifier (IOI)	20		
4.5.5	Charging function addresses	20		
5	Application usage of SIP	20		
5.1	Procedures at the UE			
5.1.1	Registration and authentication.			
5.1.1.1	<u> </u>			
5.1.1.1				
5.1.1.2				
5.1.1.3				
5.1.1.4				
5.1.1.5	· · · · · · · · · · · · · · · · · · ·			
5.1.1.5	5.1 General	25		
5.1.1.5				
5.1.1.5	Abnormal cases	27		
5.1.1.5	A Change of IP address due to privacy	27		
5.1.1.6	User-initiated deregistration	27		
5.1.1.7	Network-initiated deregistration	29		
5.1.2	Subscription and notification	29		
5.1.2.1	Notification about multiple registered public user identities	29		
5.1.2.2	General SUBSCRIBE requirements	29		
5.1.2A		29		
5.1.2A				
5.1.2A	2 Mobile-terminating case	30		
5.1.3	Call initiation - mobile originating case	31		
5.1.3.1	Initial INVITE	31		
5.1.4	Call initiation - mobile terminating case	31		
5.1.4.1	Initial INVITE	31		
5.1.5	Call release	32		
5.1.6	Emergency service			
5.1.7	Void	32		
5.2	Procedures at the P-CSCF	32		
5.2.1	General	32		
5.2.2	Registration	33		

5.2.3	Subscription to the user's registration-state event package	
5.2.4	Registration of multiple public user identities	37
5.2.5	Deregistration	37
5.2.5.1	User-initiated deregistration	37
5.2.5.2	Network-initiated deregistration	37
5.2.6	General treatment for all dialogs and standalone transactions excluding the REGISTER method	38
5.2.6.1	Introduction	38
5.2.6.2	Determination of mobile-originated or mobile-terminated case	38
5.2.6.3	Requests initiated by the UE	38
5.2.6.4	Requests terminated by the UE	41
5.2.7	Initial INVITE	44
5.2.7.1	Introduction	44
5.2.7.2	Mobile-originating case	
5.2.7.3	Mobile-terminating case	
5.2.7.4	Access network charging information	45
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	
5.2.8.1.2	Release of an existing session	
5.2.8.1.3	Abnormal cases	46
5.2.8.1.4	Release of the existing dialogs due to registration expiration and deletion of the security association	14
5.2.8.2	Call release initiated by any other entity	
5.2.8.2 5.2.9	Subsequent requests	
5.2.9.1	Mobile-originating case	
5.2.9.1	Mobile-terminating case	
5.2.9.2	Emergency service	
5.2.10	Void	
5.2.11	Procedures at the I-CSCF	
5.3.1	Registration procedure	
5.3.1.1	General	
5.3.1.2	Normal procedures	
5.3.1.3	Abnormal cases	
5.3.2	Initial requests	
5.3.2.1	Normal procedures	
5.3.2.2	Abnormal cases	
5.3.3	THIG functionality in the I-CSCF(THIG)	
5.3.3.1	General	
5.3.3.2	Encryption for topology hiding	
5.3.3.3	Decryption for Topology Hiding	
5.3.4	Void	
5.4	Procedures at the S-CSCF	
5.4.1	Registration and authentication	
5.4.1.1	Introduction	52
5.4.1.2	Initial registration and user-initiated reregistration	52
5.4.1.2.1	Unprotected REGISTER	
5.4.1.2.2	Protected REGISTER	53
5.4.1.2.3	Abnormal cases	
5.4.1.3	Authentication and reauthentication	56
5.4.1.4	User-initiated deregistration	56
5.4.1.5	Network-initiated deregistration	57
5.4.1.6	Network-initiated reauthentication.	
5.4.1.7	Notification of Application Servers about registration status	
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	
5.4.2.1.2	Notification about registration state	
5.4.3	General treatment for all dialogs and standalone transactions excluding requests terminated by the S-	
5 4 2 1	CSCF	
5.4.3.1	Determination of mobile-originated or mobile-terminated case	
5.4.3.2	Requests initiated by the served user	61 63
144	Requests terminated at the served fiser	n ·

5.4.3.4	Original dialog identifier	
5.4.3.5	Void	
5.4.4	Call initiation	
5.4.4.1	Initial INVITE	
5.4.4.2	Subsequent requests	
5.4.4.2.1	Mobile-originating case	
5.4.4.2.2	Mobile-terminating case	
5.4.5	Call release	
5.4.5.1 5.4.5.1.1	S-CSCF-initiated session release	
5.4.5.1.1	Release of an existing session	
5.4.5.1.2 5.4.5.1.2 <i>A</i>	· · · · · · · · · · · · · · · · · · ·	
5.4.5.1.2 <i>F</i> 5.4.5.1.3	Abnormal cases	
5.4.5.2	Session release initiated by any other entity	
5.4.6	Call-related requests	
5.4.6.1	ReINVITE	
5.4.6.1.1	Determination of served user	
5.4.6.1.2	Mobile-originating case	
5.4.6.1.3	Mobile-terminating case	
5.4.7	Void	
5.5	Procedures at the MGCF	
5.5.1	General	69
5.5.2	Subscription and notification	69
5.5.3	Call initiation	69
5.5.3.1	Initial INVITE	69
5.5.3.1.1	Calls originated from circuit-switched networks	69
5.5.3.1.2	Calls terminating in circuit-switched networks	69
5.5.3.2	Subsequent requests	
5.5.3.2.1	Calls originating in circuit-switched networks	
5.5.3.2.2	Calls terminating in circuit-switched networks	
5.5.4	Call release	
5.5.4.1	Call release initiated by a circuit-switched network	
5.5.4.2	IM CN subsystem initiated call release	
5.5.4.3	MGW-initiated call release	
5.5.5	Call-related requests	
5.5.5.1	ReINVITE	
5.5.5.1.1	Calls originating from circuit-switched networks	
5.5.5.1.2	Calls terminating in circuit-switched networks	
5.5.6	Further initial requests	
5.6 5.6.1	General	
5.6.2	Session initiation transaction	
5.0.2 5.7	Procedures at the Application Server (AS)	
5.7.1	Common Application Server (AS) procedures	
5.7.1.1	Notification about registration status	
5.7.1.2	Extracting charging correlation information	
5.7.1.2	Access-Network-Info	
5.7.2	Application Server (AS) acting as terminating UA, or redirect server	
5.7.3	Application Server (AS) acting as originating UA	
5.7.4	Application Server (AS) acting as a SIP proxy	
5.7.5	Application Server (AS) performing 3rd party call control	
5.7.5.1	General	
5.7.5.2	Call initiation.	
5.7.5.2.1	Initial INVITE	
5.7.5.2.2	Subsequent requests	
5.7.5.3	Call release	
5.7.5.4	Call-related requests	
5.7.5.5	Further initial requests	
5.7.6	Void	74
5.8	Procedures at the MRFC	74
5.8.1	General	74
5.8.2	Call initiation	75

5.8.2.1	Initial INVITE	75
5.8.2.1.1	MRFC-terminating case	75
5.8.2.1.1.	1 Introduction	75
5.8.2.1.2	MRFC-originating case	76
5.8.2.2	Subsequent requests	
5.8.2.2.1	Tones and announcements	
5.8.3	Call release	7 <i>6</i>
5.8.3.1	S-CSCF-initiated call release	
5.8.3.1.1	Tones and announcements	
5.8.3.2	MRFC-initiated call release	
5.8.3.2.1	Tones and announcements	
5.8.2.2.2	Transcoding	
5.8.4	Call-related requests	
5.8.4.1	ReINVITE	
5.8.4.1.1	MRFC-terminating case	
5.8.4.1.2	MRFC-originating case	
5.8.4.2	REFER	
5.8.4.2.1	MRFC-terminating case	
5.8.4.2.1	MRFC-originating case	
5.8.4.2.3	REFER initiating a new session	
5.8.4.2.4	REFER replacing an existing session	
5.8.4.3	INFO	
5.8.5	Further initial requests	
6 A	pplication usage of SDP	78
6.1	Procedures at the UE	
6.2	Procedures at the P-CSCF	
6.3	Procedures at the S-CSCF	
6.4	Procedures at the MGCF	
6.4.1	Calls originating from circuit-switched networks	
6.4.2	Calls terminating in circuit-switched networks	
6.5	Procedures at the MRFC	
6.6	Procedures at the AS	
0.0	riocedules at the As	
7 E	xtensions within the present document	81
7.1	SIP methods defined within the present document	
7.2	SIP headers defined within the present document	
7.2.0	General	
7.2.1	Void	
7.2.2	Void	
7.2.3	Void	81
7.2.4	Void	
7.2.5	Void	
7.2.6	Void	
7.2.7	Void	
7.2.7	Void	
7.2.8 7.2.9	Void	
7.2.9	Void	
7.2.10 7.2A	Extensions to SIP headers defined within the present document	
7.2A 7.2A.1		
7.2A.1 7.2A.1.1	Extension to WWW-authenticate header	
7.2A.1.2	Syntax	
7.2A.1.3	Operation	
7.2A.2	Extension to Authorization header	
7.2A.2.1	Introduction	
7.2A.2.2	Syntax	
7.2A.2.3	Operation	
7.2A.3	Tokenized-by parameter definition (various headers)	
7.2A.3.1	Introduction	
7.2A.3.2	Syntax	
7.2A.3.3	Operation	
7.2A.4	P-Access-Network-Info header	83

7.2A.4.1	Introduction	
7.2A.4.2	Syntax	
7.2A.4.3	Additional coding rules for P-Access-Network-Info header	
7.2A.5	P-Charging-Vector header	
7.2A.5.1	Introduction	
7.2A.5.2	Syntax	
7.2A.5.3	Operation	
7.2A.6	Void	
7.2A.7	Extension to Security-Client, Security-Server and Security-Verify headers	
7.2A.7.1	Introduction	
7.2A.7.2	Syntax	
7.2A.7.3	Operation	
7.3	Option-tags defined within the present document	
7.4 7.5	Status-codes defined within the present document	
7.5 7.6	Session description types defined within the present document	
7.6.1	General General	
7.6.2	Document Type Definition	
7.6.3	XML Schema description	
7.0.3 7.7	SIP timers	
7.7	IM CN subsystem timers	
	•	
8 SI	IP compression	88
8.1	SIP compression procedures at the UE	88
8.1.1	SIP compression	
8.1.2	Compression of SIP requests and responses transmitted to the P-CSCF	
8.1.3	Decompression of SIP requests and responses received from the P-CSCF	
8.2	SIP compression procedures at the P-CSCF	
8.2.1	SIP compression	
8.2.2	Compression of SIP requests and responses transmitted to the UE	
8.2.3	Decompression of SIP requests and responses received from the UE	88
9 G	PRS aspects when connected to the IM CN subsystem	89
9.1	Introduction	
9.2	Procedures at the UE	
9.2.1	PDP context activation and P-CSCF discovery	
9.2.1A	Modification of a PDP context used for SIP signalling	
9.2.1B	Re-establishment of the PDP context for signalling	
9.2.2	Session management procedures	
9.2.3	Mobility management procedures	
9.2.4	Cell selection and lack of coverage.	
9.2.5	PDP contexts for media	
9.2.5.1	General requirements	91
9.2.5.1A	Activation or modification of PDP contexts for media	91
9.2.5.2	Special requirements applying to forked responses	92
9.2.5.3	Unsucessful situations	92
Annex A	A (normative): Profiles of IETF RFCs for 3GPP usage	93
A.1 Pı	rofiles	93
A.1.1	Relationship to other specifications	
A.1.1 A.1.2	Introduction to methodology within this profile	
A.1.2 A.1.3	Roles	
	rofile definition for the Session Initiation Protocol as used in the present document	
A.2.1	User agent role	95
A.2.1.1	Introduction	
A.2.1.2	Major capabilities	
A.2.1.3	PDUs	
A.2.1.4	PDU parameters	
A.2.1.4.1		
A.2.1.4.2		
A.2.1.4.3	BYE method	102

History	261
Annex B (informative): Change history	
A.4 Profile definition for other message bodies as used in the present document	245
A.3.3.4 Void	245
A.3.3.3 Void	
A.3.3.2 SDP types	
A.3.3.1 Major capabilities	
A.3.3 Proxy role	
A.3.2.4 Void	
A.3.2.3 Void	
A.3.2.2 SDP types	
A.3.2.1 Major capabilities	
A.3.2 User agent role	
A.3.1 Introduction	
A.3 Profile definition for the Session Description Protocol as used in the present document	
A.2.2.4.14 UPDATE method	
A.2.2.4.12 REGISTER method	
A.2.2.4.11 REFER method A.2.2.4.12 REGISTER method	
A.2.2.4.10 PRACK method	
A.2.2.4.9 OPTIONS method	
A.2.2.4.8 NOTIFY method	
A.2.2.4.7A MESSAGE method	
A.2.2.4.7 INVITE method	
A.2.2.4.6 INFO method	
A.2.2.4.5 COMET method	
A.2.2.4.4 CANCEL method	
A.2.2.4.3 BYE method	
A.2.2.4.2 ACK method	
A.2.2.4.1 Status-codes	
A.2.2.4 PDU parameters	
A.2.2.3 PDUs	
A.2.2.2 Major capabilities	
A.2.2.1 Introduction	
A.2.2 Proxy role	
A.2.1.4.14 UPDATE method	
A.2.1.4.13 SUBSCRIBE method	
A.2.1.4.12 REGISTER method	
A.2.1.4.11 REFER method	141
A.2.1.3.10 PRACK method	135
A.2.1.4.9 OPTIONS method	
A.2.1.4.8 NOTIFY method	
A.2.1.4.7A MESSAGE method	
A.2.1.4.7 INVITE method	
A.2.1.4.6 INFO method	
A.2.1.4.5 COMET method	
A.2.1.4.4 CANCEL method	107

Foreword

This Technical Specification has been produced by the 3rd 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 the Media Gateway Control Function (MGCF);
- the interface between the S-CSCF and the Media Resource Function Controller (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 BGCF and any other BGCF; and
- the interface between the CSCF and an external Multimedia IP network.

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.

NOTE: The present document covers only the usage of SIP and SDP to communicate with the entitities of the IM CN subsystem. It is possible, and not precluded, to use the capabilities of GPRS 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*.
- 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
 3GPP TS 23.002: "Network architecture".
 3GPP TS 23.003: "Numbering, addressing and identification".
 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".
 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".
 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".
[8]	3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".
[9]	3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".
[9A]	3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".
[10]	3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".
[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)".
[12]	3GPP TS 29.207: "Policy control over Go interface".
[13]	3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".
[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".
[16]	3GPP TS 32.200: "Telecommunication management; Charging management; Charging principles".
[17]	3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia subsystem".
[18]	3GPP TS 33.102: "3G Security; Security architecture".
[19]	3GPP TS 33.203: "Access security for IP based services".
[20]	3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control 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]	RFC 2403 (November 1998) "The Use of HMAC-MD5-96 within ESP and AH".
[20D]	RFC 2404 (November 1998) "The Use of HMAC-SHA-1-96 within ESP and AH".
[20E]	RFC 2462 (November 1998): "IPv6 Address Autoconfiguration".
[21]	RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication".
[22]	RFC 2806 (April 2000): "URLs for Telephone Calls".
[23]	RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".
[24]	RFC 2916 (September 2000): "E.164 number and DNS".
[25]	RFC 2976 (October 2000): "The SIP INFO method".
[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)".
[28]	RFC 3265 (June 2002): "Session Initiation Protocol (SIP) Specific Event Notification".

(SIP)". RFC 3313 (January 2003): "Private Session Initiation Protocol (SIP) Extensions for Media Authorization". RFC 3320 (March 2002): "Signaling Compression (SigComp)". RFC 3323 (November 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)". RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks". RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registerin Non-Adjacent Contacts". RFC 3315 (April 2003): "The Session Initiation Protocol (SIP) REFER method". RFC 3420 (November 2002): "Internet Media Type message/sipfrag". RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Servic Route Discovery During Registration". RFC 3608 (October 2003): "Session Description Protocol". RFC 3456 (June 2006): "SDP: Session Description Protocol for IPv6 (DHCPv6)". RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers". RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SIP) static dictionary for Signaling Compression (SigComp)". RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations' Void. Void. Void. RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)". RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Usin Authentication and Key Agreement (AKA)".		
(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): "Private Extensions to the Session Initiation Protocol (SIP)" on Network Asserted Identity within Trusted Networks". [34] RFC 3325 (November 2002): "Session Initiation Protocol Extension Header Field for Registerin Non-Adjacent Contacts". [35] RFC 3327 (December 2002): "Session Initiation Protocol (SIP) REFER method". [36] RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method". [37] RFC 3420 (November 2002): "Internet Media Type message/sipfrag". [38] RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Servic 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)". [41] RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Services". [42] RFC 3485 (Pebruary 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' Void. [44] Void. [45] Void. [46] Void. [47] Void. [48] RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messagin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messagin Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [51] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)". [52] RFC 3486 (February 2003): "Session Description Protocol (SIP) Bandwidth Modifiers for RTP	[29]	RFC 3311 (September 2002): "The Session Initiation Protocol (SIP) UPDATE method".
Authorization". RFC 3320 (March 2002): "Signaling Compression (SigComp)". RFC 3323 (November 2002): "A Private Extensions to the Session Initiation Protocol (SIP)". RFC 3325 (November 2002): "Fivrate Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks". RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registerin Non-Adjacent Contacts". RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method". RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) Extension Header Field for Servic Route Discovery During Registration". RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Servic Route Discovery During Registration". RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)". RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers". RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SIP) state dictionary for Signaling Compression (SigComp)". RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations' Void. Void. Void. Void. Void. RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)". RFC 3428 (December 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication and Key Agreement (AKA)". RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messagin Void. RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". RFC 3486 (February 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) in RFC 3556 (July 2003): "Mapping of Media Streams to Resource Reservation Flows". RFC 3486 (February 2003): "Session Description Protocol (SIP) Bandwidth Modifiers for RTP	[30]	RFC 3312 (October 2002): "Integration of resource management and Session Initiation Protocol (SIP)".
RFC 3323 (November 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)". RFC 3325 (November 2002): "Brivate Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks". RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registerin Non-Adjacent Contacts". RFC 3327 (December 2002): "Internet Media Type message/sipfrag". RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method". RFC 3420 (November 2002): "Internet Media Type message/sipfrag". RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Servic Route Discovery During Registration". RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)". RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers". RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SIP) static dictionary for Signaling Compression (SigComp)". RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations' Void. Void. Void. Void. Void. RFC 3310 (September 2002): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)". RFC 3428 (December 2002): "Session Initiation Protocol (HTTP) Digest Authentication Usin Authentication and Key Agreement (AKA)". RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extensions for Instant Messagin, Void. RFC 3428 (December 2002): "Grouping of Media Lines in Session Description Protocol". RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol". RFC 3466 (February 2003): "Compressing the Session Initiation Protocol (SIP)". RFC 3466 (February 2003): "Session Description Protocol (SIP) Bandwidth Modifiers for RTP	[31]	
RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks". RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registerin Non-Adjacent Contacts". RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method". RFC 3420 (November 2002): "Internet Media Type message/sipfrag". RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Servic Route Discovery During Registration". RFC 3608 (October 2003): "Session Description Protocol". RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)". RFC 3315 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers". RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SIP) Satisfic dictionary for Signaling Compression (SigComp)". RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations' Void. Void. Void. Void. RFC 3310 (September 2002): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)". RFC 3418 (December 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Usin Authentication and Key Agreement (AKA)". SFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messagin, Void. RFC 3428 (December 2002): "Gession Initiation Protocol (SIP) Extension to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol". RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)". RFC 3486 (February 2003): "Session Description Protocol (SIP) Bandwidth Modifiers for RTP	[32]	RFC 3320 (March 2002): "Signaling Compression (SigComp)".
Network Asserted Identity within Trusted Networks". RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registerin Non-Adjacent Contacts". RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method". RFC 3420 (November 2002): "Internet Media Type message/sipfrag". RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Servic Route Discovery During Registration". RFC 3608 (October 2003): "Session Description Protocol (SIP) Extension Header Field for Servic Route Discovery During Registration". RFC 3515 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)". RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers". RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SIP) Static dictionary for Signaling Compression (SigComp)". RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations' Void. Void. Void. Void. Void. RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)". RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Usin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [51] RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol". RFC 3466 (February 2003): "Compressing the Session Initiation Protocol (SIP)". RFC 3466 (February 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP	[33]	RFC 3323 (November 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".
Non-Adjacent Contacts". [36] RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method". [37] RFC 3420 (November 2002): "Internet Media Type message/sipfrag". [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)". [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 (SIP) static dictionary for Signaling Compression (SigComp)". [43] RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations' Void. [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 Usin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messagin, Void. [51] Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)".	[34]	
[37] RFC 3420 (November 2002): "Internet Media Type message/sipfrag". [38] RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Servic 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)". [41] RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) and Session Description Protocol (SIP) static dictionary for Signaling Compression (SigComp)". [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' Void. [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 and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messagin, Void. [51] Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)".	[35]	RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".
RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Servic 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)". [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' Void. [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 Usin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [51] RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol". [52] RFC 3524 (April 2003): "Mapping of Media Streams to Resource Reservation Flows". [55] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)".	[36]	RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method".
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)". [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 (SIP) static dictionary for Signaling Compression (SigComp)". [43] RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations' Void. [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 Usin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messagin, Void. [51] Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)".	[37]	RFC 3420 (November 2002): "Internet Media Type message/sipfrag".
[40] RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)". [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' Void. [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 Usin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messagin, Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)".	[38]	RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration".
[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' Void. [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 Usin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging Void. [51] Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)". [56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP	[39]	RFC 4566 (June 2006): "SDP: Session Description Protocol".
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' Void. [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 Usin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messagin, Void. [51] Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)". [56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP	[40]	RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".
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 Usin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging Void. [51] Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)".	[41]	
 [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 Usin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging. [51] Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)". [56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP 	[42]	
[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 Usin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)".	[43]	RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".
[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 Usin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messagin, [51] Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)".	[44]	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 Usin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging Void. [51] Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)". [56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP	[45]	Void.
RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)". RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Usin Authentication and Key Agreement (AKA)". RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging Void. RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol". RFC 3524 (April 2003): "Mapping of Media Streams to Resource Reservation Flows". RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)". RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP	[46]	Void.
(SIP)". [49] RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Usin Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging Void. [51] Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)". [56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP	[47]	Void.
Authentication and Key Agreement (AKA)". [50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messagin, [51] Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)". [56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP	[48]	RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".
 [51] Void. [52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)". [56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP 	[49]	RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".
[52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)". [56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP	[50]	RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".
Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)". [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)". [56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP	[51]	Void.
 [54] RFC 3524 (April 2003): "Mapping of Media Streams to Resource Reservation Flows". [55] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)". [56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP 	[52]	
[55] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)". [56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP	[53]	RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol".
[56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP	[54]	RFC 3524 (April 2003): "Mapping of Media Streams to Resource Reservation Flows".
	[55]	RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)".
	[56]	

[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".

3 Definitions and abbreviations

3.1 Definitions

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

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 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 requirements 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].

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

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).

Back-to-Back User Agent (B2BUA)

Client

Dialog

Final response

Header

Header field

Loose routeing

Method

Option-tag (see RFC 3261 [26] subclause 19.2)

Provisional response

Proxy, proxy server

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:

Breakout Gateway Control Function (BGCF)
Call Session Control Function (CSCF)
Home Subscriber Server (HSS)
Media Gateway Control Function (MGCF)
Media Resource Function Controller (MRFC)
Subscription Locator Function (SLF)

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

Filter criteria Initial filter criteria Initial request Standalone transaction Subsequent request

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.228 [7] subclause 4.3.3.1 and subclause 4.6 apply:

Implicit registration set
Interrogating-CSCF (I-CSCF)
Policy Decision Function (PDF)
Private user identity
Proxy-CSCF (P-CSCF)
Public user identity
Serving-CSCF (S-CSCF)

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

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:

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

NOTE: A number of different security associations exist within the IM CN subsystem. Within this document the term specifically applies to the security association that exists between the UE and the P-CSCF, as this is

the only security association that has direct impact on SIP.

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

International public telecommunication 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

AS Application Server
APN Access Point Name
AUTN Authentication TokeN
B2BUA Back-to-Back User Agent

BGCF Breakout Gateway Control Function

c conditional

CCF Charging Collection Function
CDR Charging Data Record

CK Ciphering Key
CN Core Network

CSCF Call Session Control Function

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System DTD **Document Type Definition ECF Event Charging Function FODN** Fully Qualified Domain Name **GCID GPRS** Charging Identifier **GGSN** Gateway GPRS Support Node **GPRS** General Packet Radio Service Home Subscriber Server HSS

i irrelevant

I-CSCF Interrogating CSCF

ICID IM CN subsystem Charging Identifier

IK Integrity Key
IM IP Multimedia

IMS IP Multimedia core network Subsystem IMSI International Mobile Subscriber Identity

IOI Inter Operator Identifier

IP Internet Protocol IPsec IP security

IPv4 Internet Protocol version 4 IPv6 Internet Protocol version 6

ISC IP multimedia Subsystem Service Control

ISIM IMS Suscriber Identity Module

m mandatory

MAC Message Authentication Code

MCC Mobile Country Code

MGCF Media Gateway Control Function

MGW Media Gateway MNC Mobile Network Code

MRFC Multimedia Resource Function Controller MRFP Multimedia Resource Function Processor

PDP Packet Data Protocol

PLMN Public Land Mobile Network
PSTN Public Switched Telephone Network

n/a not applicable

NAI Netework Access Identifier

o optional
P-CSCF PDU Protocol Data Unit
RAND RANDom challenge

RES RESponse

RTCP Real-time Transport Control Protocol

RTP Real-time Transport Protocol

S-CSCF Serving CSCF

SDP Session Description Protocol
SGSN Serving GPRS Support Node
SIP Session Initiation Protocol
SLF Subscription Locator Function

SQN SeQuence Number UA User Agent UAC User Agent Client UAS User Agent Server UE User Equipment

UICC Universal Integrated Circuit Card
URI Universal Resource Identifier
URL Universal Resource Locator
USIM UMTS Subscriber Identity Module

x prohibited XMAC expected MAC

XML eXtensible Markup Language

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 Mg reference point, the Mi reference point, the Mj reference point, the Mm reference point, the Mr reference point and the Mw 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.

The Gm reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Mm reference point and the Mw reference point are defined in 3GPP TS 23.002 [2].

The Mr reference point is defined in 3GPP TS 23.228 [7].

The ISC interface is defined in 3GPP TS 23.228 [7] subclause 4.2.4.

- 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 dependent procedures described in subclause 9.2.
- 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 as described in subclause 5.2, 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; and
 - b) when performing P-CSCF initiated dialog-release the P-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.
- 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 provided 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 provided 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.
- NOTE 1: 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.
- NOTE 2: 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 3: 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 5.2a 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.

4.2 URI and address assignments

In order for SIP and SDP to operate, the following preconditions 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 IPv6 addresses in accordance with the constraints specified in 3GPP TS 23.221 [6] subclause 5.1.
- 3) The subscriber is allocated a private user identity by the home network operator, and this is contained within the ISIM application, if present, on the UICC. Where no ISIM application is present, the private user identity is derived from the IMSI, which is contained on the USIM (see 3GPP TS 23.003 [3]). This private user identity is available to the SIP application within the UE.

NOTE: The SIP URIs may 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. At least one of these is contained within the ISIM application, if present, on the UICC. Where no ISIM application is present, the UE

shall derive a temporary public user identity from the IMSI contained on the USIM (see 3GPP TS 23.003 [3]). All registered public user identities are available to the SIP application within the UE, after registration.

5) For the purpose of access to the IM CN subsystem, UEs are assigned IPv6 prefixes in accordance with the constraints specified in 3GPP TS 23.221 [6] subclause 5.1 (see subclause 9.2.1 for the assignment procedures).

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.

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 then initial REGISTER requests on the protected ports as described in 3GPP TS 33.203 [19].

4.3 Routeing principles of IM CN subsystem entities

Each IM CN subsystem functional entity shall apply loose routeing policy as described in RFC 3261 [26], when processing a SIP request. In cases where the I-CSCF or the S-CSCFmay interact with strict routers in non IM CN subsystem networks, the routeing procedures defined in RFC 3261 [26] that ensure interoperability with strict routers shall be used by the I-CSCF and S-CSCF.

4.4 Trust domain

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 P-CSCF, the I-CSCF, the S-CSCF, the BGCF. the MGCF, the MRFC, and all ASs that are not provided by third-party service providers. ASs provided by third-party service providers are outside the trust domain. Except when communicating with the UE, functional entities within the trust domain can safely consider that there are no requirements to take an action on the removal of the P-Asserted-Identity header, unless otherwise explicitly stated.

For the purpose of the P-Access-Network-Info header, a trust domain also applies. This trust domain is identical to that of the P-Asserted-Identity. For the P-Access-Network-Info header, subclause 5.4 also identifies additional cases for the removal of the header.

NOTE: In addition to the procedures specified in clause 5, procedures of RFC 3325 [34] in relation to transmission of P-Asserted-Identity headers and their contents outside the trust domain also apply.

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 32.200 [16] and 3GPP TS 32.225 [17] for further information on charging. The interface between the PDF and P-CSCF is not defined in this release.

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:
 - a. GPRS Charging Information;

- 3. Inter Operator Identifier (IOI);
- 4. Charging function addresses:
 - a. Charging Collection Function (CCF);
 - b. Event Charging Function (ECF).

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 as defined in subclause 7.2A.5. The P-Charging-Vector header contains the following parameters: icid, access network charging information and ioi.

The offline and online charging function addresses are encoded in the P-Charging-Function-Addresses as defined in RFC 3455 [52]. The P-Charging-Function-Addresses header contains the following parameters: CCF and ECF.

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 dialog (session) or standalone (non-session) method will generate the ICID and include it in the icid parameter of the P-Charging-Vector header in the SIP request. See 3GPP TS 32.225 [17] for requirements on the format of ICID. The P-CSCF will generate an ICID for mobile-originated calls. The I-CSCF will generate an ICID for mobile-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. 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 mobile 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. The valid duration of the ICIDis specified in 3GPP TS 32.225 [17].

The icid parameter is included in any requests that include the P-Charging-Vector header. However, the P-Charging-Vector (and ICID) is not passed to the UE.

The ICID is also passed from the P-CSCF/PDF to the GGSN, but the ICID is not passed to the SGSN. The interface supporting this operation is outside the scope of this document.

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 GPRS charging information

The GGSN provides the GPRS charging information to the IM CN subsystem, which is the common information used to correlate GGSN CDRs with IM CN subsystem CDRs. The GPRS charging information is used to correlate the bearer level (i.e. PDP context) with session level.

The GPRS charging information is generated at the first opportunity after the resources are allocated at the GGSN. The GPRS charging ingormation is passed from GGSN to P-CSCF/PDF. GPRS charging information will be updated with new information during the session as media flows are added or removed. The P-CSCF provides the GPRS charging information to the S-CSCF. The S-CSCF may also pass the information to an AS, which may be needed for online prepay applications. The GPRS charging information for the originating network is used only within that network, and similarly the GPRS charging information for the terminating network is used only within that network. Thus the GPRS charging information are not shared between the calling and called networks. The GPRS charging information is not passed towards the external ASs from its own network.

The GPRS charging information is populated in the P-Charging-Vector using the gprs-charging-info parameter. The details of the gprs-charging-info parameter is described in subclause 7.2A.5.

4.5.4 Inter operator identifier (IOI)

The Inter Operator Identifier (IOI) is a globally unique identifier to share between operator networks/service providers/content providers. There are two possible instances of an IOI to be exchanged between networks/service providers/content providers: one for the originating side, orig-ioi, and one for the terminating side, term-ioi.

The S-CSCF in the originating network populates the orig-ioi parameter of the P-Charging-Vector header in the initial request, which identifies the operator network from which the request originated. Also in the initial request, the term-ioi parameter is left out of the P-Charging-Vector header. The S-CSCF in the originating network retrieves the term-ioi parameter from the P-Charging-Vector header within the message sent in response to the initial request, which identifies the operator network from which the response was sent.

The S-CSCF in the terminating network retrieves the orig-ioi parameter from the P-Charging-Vector header in the initial request, which identifies the operator network from which the request originated. The S-CSCF in the terminating network populates the term-ioi parameter of the P-Charging-Vector header in the response to the initial request, which identifies the operator network from which the response was sent.

The MGCF takes responsibility for populating the orig-ioi parameter when a call/session is originated from the PSTN/PLMN. The MGCF takes responsibility for populating the term-ioi parameter when a call/session is terminated at the PSTN/PLMN.

IOIs will not be passed along within the network, except when proxied by BGCF and I-CSCF to get to MGCF and S-CSCF. However, IOIs will be sent to the AS for accounting purposes.

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 are to provide a common location for each entity to send charging information. Charging Collection Function (CCF) addresses are used for offline billing. Event Charging Function (ECF) addresses are used for online billing.

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

The CCF and/or ECF 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. CCF and/or ECF addresses may be allocated as locally preconfigured addresses. The AS may also retrieve the charging function address from the HSS via Sh interface.

5 Application usage of SIP

5.1 Procedures at the UE

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).

The UE shall use one IP address for all SIP signalling, i.e. simultaneous registration using different IP addresses from the same UE is not supported in this release of this document.

NOTE: The UE can use multiple Contact header parameter values simultanously, provided they all contain the same IP address and port number.

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.

5.1.1.1A Parameters contained in the UICC

If there is an ISIM and a USIM application on a UICC, then the ISIM application shall always be used for IMS authentication, as described in 3GPP TS 33.203 [19].

In case the UE is loaded with a UICC that contains the ISIM application, it will be preconfigured with all the necessary parameters to initiate the registration to the IM CN subsystem. These parameters include:

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

In case the UE is loaded with a UICC that does not contain the ISIM application, 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]. If the UICC does not contain the ISIM application, the UE shall derive new values every time the UICC is changed, and shall discard existing values if the UICC is removed.

The temporary public user identity is only used in REGISTER requests, i.e. initial registration, re-registration, mobile-initiated deregistration. After a successful registration, the UE will get the associated public user identities, and the UE may use any of them in subsequent non-REGISTER requests.

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.

5.1.1.2 Initial registration

The UE can register a public user identity at any time that a valid PDP context exists. 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.

The UE shall send only the initial 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, the UE shall send the initial REGISTER request to the SIP default port values as specified in RFC 3261 [26].

A REGISTER request may be protected using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration.

The UE shall extract or derive from the UICC 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. A public user identity may be input by the end user.

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

- a) the Authorization header, with:
 - the username directive, set to the value of the private user identity;

- the realm directive, set to the domain name of the home network;
- the uri directive, set to the SIP URI of the domain name of the home network;
- the nonce directive, set to an empty value; and
- the response directive, set to an empty value;
- b) the From header set to the SIP URI that contains the public user identity to be registered;
- c) the To header set to the SIP URI that contains the public user identity to be registered;
- d) the Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;
- e) the Via header containing the IP address or FQDN of the UE in the sent-by field. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the sent-by field.
- NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, 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 protected port value see 3GPP TS 33.203 [19].
- f) the Expires header, or the expires parameter within the Contact header, set to the value of 600 000 seconds as the value desired for the duration of the registration;
- NOTE 3: 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.
- g) a Request-URI set to the SIP URI of the domain name of the home network;
- h) the Security-Client header field set to specify the 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 HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];
- i) the Supported header containing the option tag "path"; and
- j) if a security association exists, a P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

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 value;
- b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;
- c) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header;
- d) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header;
- e) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs; and
- f) 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.

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 305 (Use Proxy) response to the initial REGISTER request, 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 a new P-CSCF discovery procedure as described in subclause 9.2.1;
- 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) too brief response to the REGISTER request, the UE shall:

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

5.1.1.3 Initial 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 users registrar (S-CSCF) as described in RFC 3680 [43].

The UE shall use the default public user identity for subscription to the registration-state event package, if the public user identity that was used for initial registration is a barred public user identity. The UE may use either the default public user identity or the public user identity used for initial registration for the subscription to the registration-state event package, if the initial public user identity that was used for initialal registration is not barred.

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 a SIP URI that contains the public user identity used for subscription;
- b) a From header set to a SIP URI that contains the public user identity used for subscription;
- c) a To header set to a SIP URI that contains the public user identity used for subscription;
- d) an Event header set to the "reg" event package;
- e) an Expires header set to 600 000 seconds as the value desired for the duration of the subscription; and
- f) a P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

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 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.

5.1.1.4 User-initiated re-registration

The UE can reregister a previously registered public user identity at any time.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less.

The UE shall protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if IK is available.

The UE shall extract or derive from the UICC 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.

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

- a) an Authorization header, with:
 - the username directive set to the value of the private user identity;
 - the realm directive, set to the value as received in the realm directive in the WWW-Authenticate header;
 - the uri directive, set to the SIP URI of the domain name of the home network;
 - the nonce directive, set to last received nonce value; and
 - the response directive, set to the last calculated response value;
- b) a From header set to the SIP URI that contains the public user identity to be registered;
- c) a To header set to the SIP URI that contains the public user identity to be registered;
- d) a Contact header set to include SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected server port value bound to the security association;
- e) a Via header containing the IP address or FQDN of the UE in the sent-by field and the protected server port value bound to the security association;
- NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, 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].
- f) an Expires header, or an expires parameter within the Contact header, set to 600 000 seconds as the value desired for the duration of the registration;
- NOTE 3: 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.
- g) a Request-URI set to the SIP URI of the domain name of the home network;
- h) a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms 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];
- i) a Security-Verify header that contains the content of the Security-Server header received in the 401 (Unauthorized) response of the last successful authentication;
- j) the Supported header containing the option tag "path"; and
- k) the P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

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

- a) store the new expiration time of the registration for this public user identity found in the To header value;
- b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;
- c) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs; and

d) set the security association lifetime to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

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 Expires header or the expires parameter with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

On receiving a 305 (Use Proxy) response to the REGISTER request, 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 a new P-CSCF discovery procedure as described in subclause 9.2.1;
- d) select a P-CSCF address, which is different from the previously used address, from the address list; and
- d) perform the procedures for initial registration as described in subclause 5.1.1.2.

5.1.1.5 Authentication

5.1.1.5.1 General

Authentication is achieved via the registration, re-registration and deregistration procedures. 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 as described in RFC 3329 [48]. If the header 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 based on the static list and parameters it received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header 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 as the shared key. The UE shall use the parameters received in the Security-Server header 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; and
- 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, with the addition that the UE shall include an Authorization header containing:
 - the realm directive set to the value as received in the realm directive in the WWW-Authenticate header;
 - the username directive, set to the value of the private user identity;

- the response directive that contains the RES parameter, as described in RFC 3310 [49];
- the uri directive, set to the SIP URI of the domain name of the home network;
- the algorithm directive, set to the value received in the 401 (Unauthorized) response; and
- the nonce directive, set to the value received in the 401 (Unauthorized) response.

The UE shall also insert the Security-Client header that is identical to the Security-Client header 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 into the request, by mirroring in it the content of the Security-Server header 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.

On receiving the 200 (OK) response for the integrity protected REGISTER request, 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
- use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

NOTE: In this case, the UE will send requests towards the P-CSCF over the newly established set of security associations. Responses towards the P-CSCF that are sent via UDP will be sent over the newly established set of security associations. 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, 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.

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 message 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 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> element 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.

5.1.1.5.3 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 directive and an empty response directive, 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 directive (see 3GPP TS 33.102 [18]).

NOTE: In the case of the SQN being out of range, a response directive 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]);
- a new Security-Client header within the REGISTER request, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup; and
- not create a temporary set of security associations.

A UE shall only respond to two consecutive invalid challenges. The UE may attempt to register with the network again after an implementation specific time.

5.1.1.5A Change of IP 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 will result in service discontinuity for IMS services.

NOTE: The procedure described below will terminate all established dialogs and transactions and temporarily disconnect the UE from the IM CN subsystem until the new registration is performed. Due to this, the UE is recommended to provide a limited use of the procedure to ensure a maximum degree of continuous service to the end user.

In order to change the IPv6 address due to privacy, the UE shall:

- 1) terminate all ongoing dialogs (e.g., sessions) and transactions (e.g., subscription to the reg event);
- 2) deregister all registered public user identities as described in subsclause 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, as follows:
 - a) by performing an initial registration as described in subsclause 5.1.1.2; and
 - b) by performing a subscription to the reg event package as described in subsclause 5.1.1.3; and
- 5) subscribe to other event packages it was subscribed to before the change of IP address procedure started.

5.1.1.6 User-initiated deregistration

The UE can deregister a previously registered public user identity at any time.

The UE shall integrity protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if one is available.

The UE shall extract or derive from the UICC 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.

Prior to sending a REGISTER request for deregistration, the UE shall release all dialogs related to the public user identity that is going to be deregistered or to one of the implicitly registered public user identities.

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

- a) the Authorization header, with;
 - the username directive, set to the value of the private user identity;
 - the realm directive, set to the value as received in the realm directive in the WWW-Authenticate header;
 - the uri directive, set to the SIP URI of the domain name of the home network;
 - the nonce directive, set to last received nonce value; and
 - the response directive, set to the last calculated response value;
- b) the From header set to the SIP URI that contains the public user identity to be deregistered;
- c) the To header set to the SIP URI that contains the public user identity to be deregistered;
- d) the Contact header 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 the protected server port value bound to the security association;
- e) a Via header containing the IP address or FQDN of the UE in the sent-by field and the protected server port value bound to the security association;
 - NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header, 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.
- f) the Expires header, or the expires parameter of the Contact header, set to the value of zero, appropriate to the deregistration requirements of the user;
- g) a Request-URI set to the SIP URI of the domain name of the home network;
- h) a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms 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];
- i) a Security-Verify header that contains the content of the Security-Server header received in the 401 (Unauthorized) response of the last successful authentication; and
- j) a P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

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.

If there are no more public user identities registered, the UE shall delete the security associations and related keys it may have towards the P-CSCF.

If all public user identities are deregistered and the security association 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 containing a value of zero).

NOTE: When the UE has received 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 (i.e. no other is registered), the UE removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY request containing the deregistration event) will not reach the UE.

5.1.1.7 Network-initiated deregistration

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) with the state attribute set to "terminated" and the event attribute set 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 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 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 contains the value of "terminated", the UE shall delete the security associations towards the P-CSCF after the server transaction (as defined in RFC 3261 [26]) pertaining to the NOTIFY request terminates.

- NOTE 1: Deleting a security association is an internal procedure of the UE and does not involve any SIP procedures.
- NOTE 2: If the security association towards the P-CSCF is removed, then the UE considers the subscription to the reg event package terminated (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero, or a NOTIFY request was received with Subscription-State header containing the value of "terminated").
- NOTE 3: When the P-CSCF has removed the security association established between the P-CSCF and the UE, further SIP signalling (e.g. the NOTIFY containing the deregistration event) will not reach the UE.

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, and the values of tags in To and From headers).

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 "terminated", i.e. deregistered is received for one or more public user identities, the UE shall store the indicated public user identities as deregistered.

NOTE: There may be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity. 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 may 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.

5.1.2.2 General SUBSCRIBE requirements

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

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

5.1.2A.1 Mobile-originating case

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

When the UE sends any request, the UE shall:

- include the protected server port in the Via header entry relating to the UE; and
- include the protected server port in any Contact header that is otherwise included.

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 5.1.1.

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

- a public user identity which has been registered by the user;
- a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implict registration that was not subsequently deregistered or has 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 1: 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.
- NOTE 2: Procedures in the network require international public telecommunication numbers when telephone numbers are used in P-Preferred-Identity header.

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the UE shall set the From header to "Anonymous".

NOTE 3: The contents of the From header should not be relied upon to be 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 may well have privacy requirements, terminal manufacturers should not automatically derive and include values in this header 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 other than Anonymous.

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].

The UE shall insert a P-Access-Network-Info header 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. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (containing the IP address or the FQDN learnt through the P-CSCF discovery procedures, and the protected port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or reregistration.

5.1.2A.2 Mobile-terminating case

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

When the UE sends any response, the UE shall:

- include the protected server port in any Contact header that is otherwise included.

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 5.1.1.

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 1: In the mobile-terminating case, this version of the document makes no provision for the UE to provide an P-Preferred-Identity in the form of a hint.

The UE shall insert a P-Access-Network-Info header 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. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

5.1.3 Call initiation - mobile originating case

5.1.3.1 Initial INVITE

Upon generating an initial INVITE request, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism;
- indicate the requirement of precondition and specify it using the Require header mechanism.

NOTE: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261. While proxies in the IM CN subsystem do not fork requests, proxies external to the system may initiate forking, such that the UE is able to receive several forked provisional or final responses from different terminations. The UE may 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.

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 further 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.

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

If the UE receives a 488 (Not Acceptable Here) response to an initial INVITE request, the UE should send a new INVITE request containing SDP according to the procedures defined in subclause 6.1.

If the UE receives a 420 (Bad Extension) response to an initial INVITE request with "precondition" option-tag in the Unsupported header field, the UE shall abort the session attempt and shall not resend this INVITE request without "precondition" option-tag in the Require header.

NOTE: An example of where a new request would not be built is where knowledge exists within the UE, or interaction occurs with the user, such that it is known that the resultant SDP would describe a session that did not meet the user requirements.

5.1.4 Call initiation - mobile terminating case

5.1.4.1 Initial INVITE

Upon receiving an initial INVITE request without containing either Supported: precondition or Require: precondition header values, the UE shall generate a 421 (Extension Required) response indicating the required extension in the Require header field.

Upon generating the first response to the initial INVITE request, the UE shall indicate the requirement for reliable provisional responses and specify it using the Require header mechanism. The UE shall send the 200 (OK) response to the initial INVITE request only after the local resource reservation has been completed.

NOTE: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261. While proxy support of forking is precluded in the IM CN subsystem, proxies external to the system may initiate forking, such that the UE is able to receive several forked requests for the same transaction.

5.1.5 Call release

Void.

5.1.6 Emergency service

A UE shall not attempt to establish an emergency session via the IM CN Subsystem when the UE can detect that the number dialled is an emergency number. The UE shall use the CS domain as described in 3GPP TS 24.008 [8].

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a 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 7.7AA), the UE shall automatically:

- send an ACK request to the P-CSCF as per normal SIP procedures;
- attempt an emergency call setup according to the procedures described in 3GPP TS 24.008 [8].

The UE may also provide an indication to the user based on the text string contained in the <reason> child element included in the "> child element included in the <i ms-3gpp> element."> element included in the <i ms-3gpp> element.

As a consequence of this, a UE operating in MS operation mode C cannot perform emergency calls.

5.1.7 Void

5.2 Procedures at the P-CSCF

5.2.1 General

The P-CSCF shall support the Path and Service-Route headers.

NOTE 1: The Path header is only applicable to the REGISTER request and its 200 (OK) response. The Service-Route header is only applicable to the 200 (OK) response of REGISTER request.

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 headers, if present.

When the P-CSCF receives any request or response from the UE, the P-CSCF shall:

- remove the P-Charging-Function-Addresses and P-Charging-Vector headers, if present. Also, the P-CSCF shall ignore any data received in the P-Charging-Function-Addresses and P-Charging-Vector headers; and
- may insert previously saved values into the P-Charging-Function-Addresses and P-Charging-Vector headers before forwarding the message.
- NOTE 2: When the P-CSCF is located in the visited network, then it will not receive the P-Charging-Function-Addresses header from the S-CSCF or I-CSCF. Instead, the P-CSCF discovers charging function addresses by other means not specified in this document.

When the P-CSCF receives any request or response containing the P-Media-Authorization header from the S-CSCF, the P-CSCF shall remove the header.

NOTE 3: If service based local policy applies, the P-CSCF will insert the P-Media-Authorization header as described in subclauses 5.2.7.2 and 5.2.7.3.

NOTE 4: The P-CSCF will integrity protect all SIP messages sent to the UE outside of the registration and authentication procedures. The P-CSCF will discard any SIP message that is not integrity protected and is received outside of the registration and authentication procedures. The integrity protection and checking requirements on the P-CSCF within the registration and authentication procedures are defined in subclause 5.2.2.

5.2.2 Registration

The P-CSCF shall be prepared to receive only the initial REGISTER requests on the SIP default port values as specified in RFC 3261 [26]. The P-CSCF shall also be prepared to receive the initial REGISTER requests on the port advertised to the UE during the P-CSCF discovery procedure.

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall:

- 1) insert a Path header 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 to the P-CSCF) are expected to be treated as for the mobile-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;
- 2) insert a Require header containing the option tag "path";
- 3) insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17];
- 4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity 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";
- 5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the 'secagree' item from the Require header, and the header itself if this is the only entry. If the header is not present, then the P-CSCF shall return a suitable 4xx response;
- 6) 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, then the request is expected to contain a Security-Verify header in addition to a Security-Client header. 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 with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header 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, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;
 - 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 if it is present, and the "sec-agree" item from the Require header, and the header itself if this is the only entry;
 - a Security-Client header containing new parameter values is expected. If this header or any required parameter is missing, then the P-CSCF shall return a suitable 4xx response;
 - the P-CSCF shall remove and store the Security-Client header before forwarding the request to the S-CSCF; and
 - c) check if the private user identity conveyed in the Authorization header of the integrity-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;

- 7) 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; and
- 8) determine the I-CSCF of the home network and forward the request to that I-CSCF.

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 values contained in the 401 (Unauthorized) response and bind them 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 have been removed;
- 3) insert a Security-Server header in the response, containing the P-CSCF static 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 HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms;
- 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. 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.
- NOTE 1: 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, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

- 1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routeing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;
- 2) associate the Service-Route header list with the registered public user identity;
- 3) store the public user identities found in the P-Associated-URI header value, and associate them to the public user identity under registration;
- 4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;
- NOTE 2: There may be more then one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.
- 5) store the values received in the P-Charging-Function-Addresses header;
- 6) 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;
- 7) if a set of temporary 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
- 8) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

When receiving 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 lifetime of the old set of security associations towards the same UE to 64*T1 (if currently longer than 64*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 3: In this case, the P-CSCF will send requests 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 4: 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 3).

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;
- 3) delete, if existing, any other set of security associations towards this UE immediately; and,
- 4) go on using for further requests sent towards the UE the set of security associations that was used to protect the REGISTER request that initiated the re-authentication.

When sending the 200 (OK) respone for a REGISTER request that concludes an initial authentication, i.e. the initial REGISTER request was received unprotected, the P-CSCF shall:

- 1) keep the newly established set of security associations created during this authentication;
- 2) delete, if existing, any other set of security associations towards this UE immediately; and,
- 3) use the kept newly established set of security associations for further messages sent towards the UE.
- NOTE 5: The P-CSCF will maintain two Route header lists. The first Route header list created during the registration procedure is used only to validate the routeing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list constructed from the Record Route headers in the initial INVITE and associated response is used during the duration of the call. Once the call is terminated, the second Route list 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

	Temporary set of security associations	Newly established set of security associations	Old set of security associations
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*T1, if lifetime is larger than 64*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*T1	No action	Take into use	No action
Sending an authorization challenge within a 401 (Unauthorized) response for a REGISTER request	Create 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 reauthentication was received. 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

5.2.3 Subscription to the user's registration-state event package

Upon receipt of a 200 (OK) response to the initial REGISTER request of an user, the P-CSCF shall subscribe to the reg event package at the users registrar (S-CSCF) as described in RFC 3680 [43]. The P-CSCF shall:

- 1) generate a SUBSCRIBE request with the following elements:
 - a Request-URI set to the resource to which the P-CSCF wants to be subscribed to, i.e. to a SIP URI that contains the default public user identity of the user;
 - a From header set to the P-CSCF's SIP URI;
 - a To header, set to a SIP URI that contains the default public user identity of the user;
 - an Event header set to the "reg" event package;
 - an Expires header set to a value higher then the Expires header indicated in the 200 (OK) response to the REGISTER request;
 - a P-Asserted-Identity header set to the SIP URI of the P-CSCF, which was inserted into the Path header during the registration of the user to whose registration state the P-CSCF subscribes to; and
 - a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17]; and
- 2) determine the I-CSCF of the home network (e.g., by using DNS services);

before sending the SUBSCRIBE request to that I-CSCF, according to the procedures of RFC 3261 [26].

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 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.

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, and the values of tags in To and From headers).

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

- if a state attribute "active", i.e. registered, is received for one or more public user identities, the P-CSCF shall
 - bind the indicated public user identities as registered to the contact information of the user; and
 - add the public user identity to the list of the public user identities that are registered for the user.
- if a state attribute "terminated", i.e. deregistered, is received for one or more public user identities, the P-CSCF shall release all stored information for these public user identities and remove these public user identities from the list of the public user identities, that are registered for the user.

NOTE: There may 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), it shall check the value of the Expires header field and/or expires parameter in the Contact header field. When the value of the Expires header field or expires parameter equals zero, then the P-CSCF shall:

- 1) remove the public user identity found in the To header field, and all the associated public user identities, from the registered public user identities list and all related stored information; and
- 2) check if the user has left any other registered public user identity. When all of the public user identities of a user are deregistered, the P-CSCF shall delete the security associations towards that user 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 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 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 (i.e. no other is registered), the P-CSCF removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (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 as described in subclause 5.2.3, including one or more <registration> element(s) with the state attribute set to "terminated" the P-CSCF shall remove all stored information for these public user identities and remove these public user identities from the list of the public user identities that are registered for the user.

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 set to "terminated", the P-CSCF shall shorten the security associations towards the UE.

- NOTE 1: The security association between the P-CSCF and the UE is shortened to a duration that will allow the NOTIFY request containing the deregistration event to reach the UE.
- NOTE 2: When the P-CSCF receives the NOTIFY request with Subscription-State header 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 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 mobile-originated or mobile-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 mobile-terminating case as described in subclause 5.2.6.4 if the request makes use of the information for mobile-terminating calls, which was added to the Path header 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 contains a specific user part or parameter;
- perform the procedures for the mobile-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

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that matches one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains as P-Preferred-Identity header that does not match one of the registered public user identities, or does not contain a P-Preferred-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity. If there is more then one default public user identity available, the P-CSCF shall randomly select one of them.

NOTE 1: The contents of the From header do not form any part of this decision process.

When the P-CSCF receives from the UE an initial request for a dialog, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or reregistration) matches the preloaded Route headers 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-CSCFshall 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 value in the request with the value of the Service-Route header received during the last 200 (OK) response for a registration or reregistration;
- 2) add its own address to the Via header. The P-CSCF Via header 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;
- 3) add its own SIP URI to the top of the Record-Route header. The P-CSCF SIP URI is built 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;
- 4) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;
- 5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17]; and
- 6) 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;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) store the values received in the P-Charging-Function-Addresses header;
- 2) store the list of Record-Route headers 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) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and
- NOTE 2: 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 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].

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 relates 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;
 - 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;
- 2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. 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 value in the request with the stored list of Record-Route headers for the same dialog;
- 3) add its own address to the Via header. The P-CSCF Via header 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) add its own SIP URI to the top of Record-Route header. The P-CSCF SIP URI is built 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; and
- 5) for INVITE dialogs (i.e. dialogs initiated by an INVITE request), replace the saved Contact and Cseq header filed values received in the request such that the P-CSCF is able to release the session if needed;
- NOTE 3: 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, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) store the list of Record-Route headers from the received response;
- 2) rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC 3486 [55]; and
- NOTE 3: 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 value see 3GPP TS 33.203 [19].
- 3) replace the saved Contact 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].

When the P-CSCF receives from the UE the request for a standalone transaction, and a Service-Route header list exists for the initiator of the request, the P-CSCF shall:

- 1) verify that the list of URIs received in the Service-Route header (during the last successful registration or reregistration) matches the preloaded Route headers 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-CSCFshall 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 value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response;
- 2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request; and
- 3) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17];

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

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;

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

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 relates 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;
 - 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;

- 2) verify that the list of Route headers in the request matches the stored list of Record-Route headers for the same dialog. 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 value in the request with the stored list of Record-Route headers for the same dialog; and
- 3) for dialogs that are not INVITE dialogs, add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17];
- 4) for INVITE dialogs, replace the saved Cseq header 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,) in accordance with the procedures of RFC 3261 [26].

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 header list exists for the initiator of the request, the P-CSCF shall:

- verify that the list of URIs received in the Service-Route header (during the last successful registration or reregistration) is included, preserving the same order, as a subset of the preloaded Route headers 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 value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response; and
- 2) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26].

5.2.6.4 Requests terminated by the UE

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) remove its own SIP URI from the topmost Route header;
- 2) convert the list of Record-Route header values into a list of Route header values and save this list of Route headers:
- 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) add its own SIP URI to the top of the list of Record-Route headers and save the list. The P-CSCF SIP URI is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association 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 established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;
- 5) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association 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 established from the UE to the P-CSCF; or
- b) the P-CSCF IP address of the security association 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 of the usage of the two ports see 3GPP TS 33.203 [19].
- 6) remove and store the values received in the P-Charging-Function-Addresses header;
- 7) remove and store the icid parameter received in the P-Charging-Vector header; and
- 8) save a copy of the P-Called-Party-ID header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

- 1) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with the value saved from the P-Called-Party-ID header that was received in the request;
- 2) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header 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 values with those received in the request;
- 3) verify that the list of URIs received in the Record-Route header of the request corresponding to the same dialog is included, preserving the same order, as a subset of the Record-Route header 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 values with those received in the request, rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter.
 - If the verification is successful, the P-CSCF shall rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;
- 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;

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 headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header 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 values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

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) remove its own SIP URI from the topmost Route header value;

- 2) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association 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 established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association established from the UE to the P-CSCF; and
- NOTE 2: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].
- 3) for INVITE dialogs, replace the saved Contact and Cseq header filed values received in the request such that the P-CSCF is able to release the session if needed;
- NOTE 3: 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 RFC 3261 [26].

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 headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header 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 values with those received in the request;
- 2) rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter; and
- 3) replace the saved Contact header field values received in the response such that the P-CSCF is able to release the session if needed;

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 headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header 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 values with those received in the request; and
- 2) rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

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) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association 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 established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association 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. For details of the usage of the two ports see 3GPP TS 33.203 [19].

- 2) store the values received in the P-Charging-Function-Addresses header; and
- 3) remove and store the icid parameter received in the P-Charging-Vector header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- 1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header 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 values with those received in the request; and
- 2) remove the P-Preferred-Identity header, if present, and insert an P-Asserted-Identity header with the value saved from Request-URI of the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

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) add its own address to the top of the received list of Via header and save the list The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC 3486 [55], and the protected server port number of the security association 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 established from the UE to the P-CSCF; or
 - b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;
- NOTE 4: The P-CSCF associates two ports, a protected client port and a protected server port, with each pair of security associations. For details of the usage of the two ports see 3GPP TS 33.203 [19].
- 2) remove and store the icid parameter from P-Charging-Vector header; and
- 3) for INVITE dialogs, replace the saved Cseq header 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 in accordance with the procedures of RFC 3261 [26].

When the P-CSCF receives any response to the above request, the P-CSCF shall:

- 1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header 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 values with those received in the request;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

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 Mobile-originating case

The P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

Upon receiving a response as specified in RFC 3313 [31] to the initial INVITE request, the P-CSCF shall:

- if a media authorization token is generated by the PDF (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

NOTE: Typically, the first 183 (Session Progress) response contains an SDP answer including one or more "m=" media descriptions, but it is also possible that the response does not contain an SDP answer or the SDP does not include at least an "m=" media description. However, the media authorization token is generated independently of the presence or absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value. The same media authorization token is used until the session is terminated.

When the P-CSCF sends the UPDATE request towards the S-CSCF, the P-CSCF shall also include the access-network-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the access network charging information.

5.2.7.3 Mobile-terminating case

When the P-CSCF receives an initial INVITE request destined for the UE, it will contain the URI of the UE in the Request-URI, and a single preloaded Route header. The received initial INVITE request will also have a list of Record-Route headers. Prior to forwarding the initial INVITE to the URI found in the Request-URI, the P-CSCF shall:

- if a media authorization token is generated by the PDF as specified in RFC 3313 [31] (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

NOTE: Typically, the initial INVITE request contains an SDP offer including one or more "m=" media descriptions, but it is also possible that the INVITE request does not contain an SDP offer or the SDP does not include at least an "m= media description. However, the media authorization token is generated independently of the presence or absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value. The same media authorization token is used until the session is terminated.

In addition, the P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

When the P-CSCF sends 180 (Ringing) or 200 (OK) (to INVITE) towards the S-CSCF, the P-CSCF shall also include the access-network-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the access network charging information.

5.2.7.4 Access network charging information

The P-CSCF shall include the access-network-charging-info parameter within the P-Charging-Vector header 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 coverage is no longer available for a served user, for whom one ore more ongoing multimedia session are currently being established, the P-CSCF shall cancel the related dialogs by sending out a CANCEL request according to the procedures described in RFC 3261 [26].

5.2.8.1.2 Release of an existing session

Upon receipt of an indication that the radio interface resources are no longer available for a served user, for whom one or more ongoing session exists, the P-CSCF shall release each of the related dialogs by applying the following steps:

- 1) if the P-CSCF serves the calling user of a session it shall generate a BYE request based on the information saved for the related dialog, including:
 - a Request-URI, set to the stored Contact header provided by the called user;
 - 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 current CSeq value stored for the direction from the calling to the called user, incremented by one;
 - a Route header, set to the routeing information towards the called user as stored for the dialog;
 - further headers, based on local policy or the requested session release reason.
- 2) If the P-CSCF serves the called user of a session it shall generate a BYE request based on the information saved for the related dialog, including:
 - a Request-URI, set to the stored Contact header provided by the calling user;
 - a To header, set to the From header value as received in the initial INVITE request;
 - a From header, set to the To header value as received in the 200 (OK) response for 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 current CSeq value stored for the direction from the called to the calling user, incremented by one;
 - a Route header, set to the routeing information towards the calling user as stored for the dialog;
 - further headers, based on local policy or the requested session release reason.
- 3) send the so generated BYE request towards the indicated user.
- 4) upon receipt of the 2xx responses for the BYE request, 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

If there are still active dialogs associated with the user after the security associations 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: At the same time, the P-CSCF will also indicate via the Go interface that all resources associated with these dialogs should be released.

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, it shall delete all the stored information related to the dialog.

5.2.9 Subsequent requests

5.2.9.1 Mobile-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 when sending the SIP request to the S-CSCF. See subclause 5.2.7.4 for further information on the access network charging information.

5.2.9.2 Mobile-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. See subclause 5.2.7.4 for further information on the access network charging information.

5.2.10 Emergency service

The P-CSCF shall store a configurable list of local emergency numbers and emergency URIs, i.e. those used for emergency services by the operator to which the P-CSCF belongs to. In addition to that, the P-CSCF shall store a configurable list of roaming partners' emergency numbers and emergency URIs associated with MCC and MNC codes.

NOTE: Certain SIP URIs may be classified as emergency URIs in all networks.

The P-CSCF shall inspect the Request URI of all INVITE requests from the UE for known emergency numbers and emergency URIs from these configurable lists. If the P-CSCF detects that the Request-URI of the INVITE request matches one of the numbers in any of these lists, the P-CSCF shall not forward the INVITE request. If support for the 3GPP IMS XML body in the Accept header is not indicated, it shall be assumed that the UE supports version 1 of the XML Schema for the IM CN subsystem XML body. The P-CSCF shall respond the INVITE request with a 380 (Alternative Service) response.

In order to determine whether the INVITE request is destined for an emergency centre in the roaming country (i.e. the list of roaming partners' are inspected), the P-CSCF shall compare the MCC and the MNC fields in the received in the P-Access-Network-Info header of the INVITE request against its own MCC and MNC codes.

The P-CSCF shall include in the 380 (Alternative Service) response:

 a Content-Type header field with the value set to associated MIME type of the 3GPP IMS XML body as described in subclause 7.6.1.

The P-CSCF shall include in the 3GPP IMS 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:
 - 1) a <type> child element, set to "emergency" (see table 7.7AA) to indicate that it was an emergency call; and
 - 2) a <reason> child element, set to an operator configurable reason.

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 I-CSCF receives a REGISTER request, the I-CSCF starts the user registration status query procedure to the HSS as specified in 3GPP TS 29.228 [14].

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].

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) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 3) forward the REGISTER request to the indicated S-CSCF.

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 then 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) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 4) forward the REGISTER request to the selected S-CSCF.

When the I-CSCF receives a 2xx response to a REGISTER request, the I-CSCF shall proxy 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 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;

and:

- the REGISTER request did not include an "integrity-protected" parameter in the Authorization header; or
- did include an "integrity-protected" parameter with a value different from "yes" in the Authorization header;

the I-CSCF performs the user registration status query procedure with the HSS as described in subclause 5.3.1.2, and based on the capabilities indicated from the HSS, the I-CSCF shall select new S-CSCF. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same registration procedure.

If a selected S-CSCF does not respond to a REGISTER request and its retransmissions by the I-CSCF and the REGISTER request did include an Authorization header with the "integrity-protected" parameter set to "yes", the I-CSCF shall send back a 408 (Request Timeout) response or 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.

When the I-CSCF receives an initial request for a dialog or standalone transaction, that does not contain a Route header, the I-CSCF shall start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [14] for the called user, indicated in 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].

Upon successful user location query, when the response contains the URI of the assigned S-CSCF, the I-CSCF shall:

- 1) insert the URI received from the HSS as the topmost Route header;
- 2) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. If no icid parameter was found, then create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header;
- 3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 4) forward the request based on the topmost Route header.

Upon successful user location query, when the response contains information about the required S-CSCF capabilities, the I-CSCF shall:

- 1) select a S-CSCF according to the method described in 3GPP TS 29.228 [14];
- 2) insert the URI of the selected S-CSCF as the topmost Route header field value;
- 3) 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); and
- 4) forward the request to the selected S-CSCF.

Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, the I-CSCF shall 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) 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 pointing to itself, the I-CSCF shall determine from the entry in the Route header whether it needs to do HSS query or hiding. In case HSS query is needed, then the I-CSCF shall perform the procedures described for the case when there is no Route header present. If the I-CSCF determines that hiding must be performed, then the THIG functionality in I-CSCF received an outgoing initial request for which topology hiding has to be applied, and the I-CSCF shall:

1) remove its own SIP URI from the topmost Route header;

- 2) perform the procedures described in subclause 5.3.3; and
- 3) route the request based on the Request-URI header field.

When the I-CSCF receives an initial request for a dialog or standalone transaction containing more than one Route header, the I-CSCF shall:

- 1) remove its own SIP URI from the topmost Route header;
- 2) apply the procedures as described in subclause 5.3.3; and
- 3) forward the request based on the topmost Route header.

NOTE: In accordance with SIP the I-CSCF can add its own routeable SIP URI to the top of the Record-Route header to any request, independently of whether it is an initial request, or whether topology hiding is performed. The P-CSCF will ignore any Record-Route header that is not in the initial request of a dialog.

When the I-CSCF receives a response to an initial request (e.g. 183 or 2xx), the I-CSCF shall store the values from the P-Charging-Function-Addresses header, if present. If the next hop is outside of the current network, then the I-CSCF shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

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.

If the HSS sends 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 with a 200 OK;
- shall answer the original request with a 487 Request Terminated; and
- shall silently discard the later arriving (pending) Cx answer message from the HSS.

5.3.3 THIG functionality in the I-CSCF(THIG)

5.3.3.1 General

The following procedures shall only be applied if topology hiding is required by the network. The network requiring topology hiding is called the hiding network.

NOTE 1: Requests and responses are handled independently therefore no state information is needed for that purpose within an I-CSCF(THIG).

The I-CSCF(THIG) shall apply topology hiding to all headers which reveal topology information, such as Via, Route, Record-Route, Service-Route.

Upon receiving an incoming REGISTER request for which topology hiding has to be applied and which includes a Path header, the I-CSCF(THIG) shall add the routeable SIP URI of an I-CSCF(THIG) to the top of the Path header. The I-CSCF(THIG) may include in the inserted SIP URI an indicator that identifies the direction of subsequent requests received by the I-CSCF i.e., from the S-CSCF towards the P-CSCF, to identify the mobile-terminating case. The I-CSCF(THIG) 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 2: Any subsequent request that includes the direction indicator (in the Route header) 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 topology hiding has to be applied and which includes a Record-Route header, the I-CSCF(THIG) shall add its own routeable SIP URI to the top of the Record-Route header.

Upon receiving an outgoing initial request for which topology hiding has to be applied and which includes P-Charging-Function-Addresses header, the I-CSCF(THIG) shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

5.3.3.2 Encryption for topology hiding

Upon receiving an outgoing request/response from the hiding network the I-CSCF (THIG) shall perform the encryption for topology hiding purposes, i.e. the I-CSCF (THIG) shall:

- 1) use the whole header 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 headers subject to encryption when performing encryption;
- 3) use for one encrypted string all received consecutive header entries subject to encryption, regardless if they appear in separate consecutive headers or if they are consecutive entries in a comma separated list in one header;
- 4) construct a hostname that is the encrypted string, and the realm is the name of the encrypting network;
- 5) append a "tokenized-by" 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 out of the resulting NAI, e.g. prepend "SIP/2.0/UDP" for Via headers or "sip:" for Route and Record-Route headers;
- 7) if the I-CSCF (THIG) encrypted an entry in the Route header, then it also inserts its own URI before the topmost encrypted entry; and
- 8) if the I-CSCF (THIG) encrypted an entry in the Via header, 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 are encrypted, they will result in only one encrypted header entry. For example:

NOTE 2: If multiple entries of the same network are within the same type of headers, but they are not consecutive, then these entries will be tokenized to different strings. For example:

NOTE 3: If request will return to the hiding network (e.g. after visiting an AS), then I-CSCF (THIG) URI is inserted. For example:

5.3.3.3 Decryption for Topology Hiding

Upon receiving and incoming requests/response to the hiding network the I-CSCF(THIG) shall perform the decryption for topology hiding purposes, i.e. the I-CSCF shall:

- 1) identify hostnames encrypted by the network this I-CSCF belongs to within all headers of the incoming message;
- 2) use those hostnames that carry the identification of the hiding network within the value of the "tokenized-by" parameter as input to decryption;

- 3) use as encrypted string the hostname which follows the sent-protocol (for Via Headers, e.g. "SIP/2.0/UDP") or the URI scheme (for Route and Record-Route Headers, e.g. "sip:");
- 4) replace all content of the received header which carries encrypted information with the entries resulting from decryption.

EXAMPLE: An encrypted entry to a Via header 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 routeing 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.

5.3.4 Void

5.4 Procedures at the S-CSCF

5.4.1 Registration and authentication

5.4.1.1 Introduction

The S-CSCF shall act as the SIP registrar for all UAs of the IM CN subsystem with public user identities.

The S-CSCF shall support the use of the Path and Service-Route header. The S-CSCF must also support the Require and Supported headers. The Path header is only applicable to the REGISTER request and its 200 (OK) response. The Service-Route header is only applicable to the 200 (OK) response of REGISTER.

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.

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Unprotected REGISTER

NOTE 1: Any REGISTER request sent unprotected by the UE is considered to be an initial registration. A 200 (OK) final response to such a request 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 2: A REGISTER with Expires header value equal to zero should always be received protected. However, it is possible that in error conditions a REGISTER with Expires header value equal to zero may be received unprotected. In that instance the procedures below will be applied.

When the S-CSCF receives a new unprotected registration request for a public 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 an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no"', for the received public user identity; and
- 2) if the authentication has been successful and if the previous registration has not expired, the S-CSCF shall perform the network initiated de-registration procedure only for the previous contact information as described in subclause 5.4.1.5.

When S-CSCF receives a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "no" and a non-empty response directive, the S-CSCF shall ignore the value of the response directive.

Upon receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no", the S-CSCF shall:

- 1) identify the user by the public user identity as received in the To header and the private user identity as received in the username field in the Authorization header of the REGISTER request;
- 2) check if the P-Visited-Network-ID header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;
- select an authentication vector for the user. If no authentication vector for this user is available, after the S-CSCF has performed the Cx Multimedia Authentication procedure with the HSS, as described in 3GPP TS 29.229 [15], the S-CSCF shall select an authentication vector as described in 3GPP TS 33.203 [19].

Prior to performing Cx Multimedia 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];

- NOTE 3: 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) store the icid parameter received in the P-Charging-Vector header;
- 5) challenge the user by generating a 401 (Unauthorized) response for the received REGISTER request, including a WWW-Authenticate header which transports:
 - a globally unique name of the S-CSCF in the realm field;
 - the RAND and AUTN parameters and optional server specific data for the UE in the nonce field;
 - the security mechanism, which is AKAv1-MD5, in the algorithm field;
 - the IK (Integrity Key) parameter for the P-CSCF in the ik field (see subclause 7.2A.1); and
 - the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2A.1);
- 6) 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;
- 7) send the so generated 401 (Unauthorized) response towards the UE; and,
- 8) 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.

5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall identify the user by the public user identity as received in the To header and the private user identity as received in the Authorization header of the REGISTER request, and:

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" parameter in the Authorization header 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 an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall check whether the public user identity received in the To header is already registered. If it is not registered, the S-CSCF shall proceed beginning with step 5 below. Otherwise, the S-CSCF shall 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 is included, containing:
 - a) the private user identity of the user in the username field;
 - b) the algorithm which is AKAv1-MD5 in the algorithm field; and
 - c) the authentication challenge response needed for the authentication procedure in the response 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 (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;
- 5) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], store the following information in the local data:
 - a) the list of public user identities associated to the public user identity under registration, including the own public user identity under registration and the implicitly registered 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;
- NOTE 1: 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 may belong to different service profiles.
- 6) bind to each non-barred registered public user identity all registered contact information and store the related method tag values from the Contact header for future use;
- NOTE 2: There might be more then one contact information available for one public user identity.
- NOTE 3: The barred public user identities are not bound to the contact information.
- 7) 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 Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;
- NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.
- 8) determine the duration of the registration by checking the value of the Expires header 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;

9) store the icid parameter received in the P-Charging-Vector header;

10) create a 200 (OK) response for the REGISTER request, including:

- a) the list of received Path headers;
- b) a P-Associated-URI header containing the list of public user identities that are associated to the public user identity under registration. 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 an already registered public user identity. The S-CSCF shall place the default public user identity as a first entry in the list of URIs present in the P-Associated-URI header. The default public user identity will be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header, as described in subclause 5.2.6.3. The S-CSCF shall not add a barred public user identity to the list of URIs in the P-Associated-URI header;
- c) a Service-Route header containing:
 - the SIP URI identifying the S-CSCF containing an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) are treated as for the mobile-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; and,
 - if network topology hiding is required a SIP URI identifying an I-CSCF(THIG) as the topmost entry; and
- d) a P-Charging-Function-Addresses header 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;
- 11) send the so created 200 (OK) response to the UE;
- 12) 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; and,
- NOTE 5: If this registration is a reregistration, the Filter Criteria already exists in the local data.
- NOTE 6: 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.
- 13) handle the user as registered for the duration indicated in the Expires header.

5.4.1.2.3 Abnormal cases

In the case that the REGISTER request that contains the authentication challenge response received from the UE does not match with the expected REGISTER request (e.g. wrong Call-Id, wrong authentication challenge response) and the request has the "integrity-protected" parameter in the Authentication header 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 time 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 no authentication challenge response and no AUTS 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 time 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 directive, 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 AUTS directive 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.
- NOTE 3: Since the UE responds only to two consecutive challenges, the S-CSCF will send a 401 (Unauthorized) response that contains a new challenge only twice.
- NOTE 4: In the case of an AUTS directive being present in the REGISTER request, the response directive in the same REGISTER request will not be taken into account by the S-CSCF.

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 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 more than one SIP URIs as Contact header entries, the S-CSCF shall only store the entry with the highest "q" value and include it in the 200 (OK) response.

NOTE 5: 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 as registered described in 3GPP TS 33.203 [19]. The operator's policy will specify when will, upon authentication failure, the currently registered public user identity or the user be de-registered by the S-CSCF.

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

When S-CSCF receives a REGISTER request with the Expires header field containing the value zero, the S-CSCF shall:

- check whether the "integrity-protected" parameter in the Authorization header field is 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" parameter is set to "yes";
- release each multimedia session that includes this user, where the session was initiated with the public user identity found in the P-Asserted-Identity header field or with one of the implicitly registered public used identities by applying the steps listed in subclause 5.4.5.1.2;
- deregister the public user identity found in the To header field together with the implicitly registered public user identities;
- 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; and
- 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, where the session was initiated with the public user identity currently registered or with one of the implicitly registered public used identities, release each of these multimedia sessions user by applying the steps listed in subclause 5.4.5.1.2.

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 containing a value of zero).

If the Authorization header of the REGISTER request did not contain an "integrity-protected" parameter, or the "integrity-protected" parameter was 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 Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], 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 of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber).

5.4.1.5 Network-initiated deregistration

Prior to initiating the network-initiated deregistration while there are still active multimedia sessions that are associated with this user, 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 (i.e. S-CSCF will set the event attribute within the <contact> element to "rejected" for the NOTIFY request, as described below), the S-CSCF shall release all sessions that are associated with the public user identities being deregistered, which includes the implicitly registered public user identities.
- when the S-CSCF expects the UE to reregister (i.e. S-CSCF will set the event attribute within the <contact> element to "deactivated" for the NOTIFY request, as described below), the S-CSCF shall only release sessions that currently include the user, where the session was initiated with the one of the public user identities being deregistered, which includes the implicitly registered public user identities.

When a network-initiated deregistration event occurs for one or more public user identity, 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 to the saved route information during subscription;
- 2) set the Event header 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 the <contact> sub-element of each <registration> element to the contact address provided by the UE;
 - b) if the public user identity:
 - i) has been deregistered then:
 - set the state attribute within the <registration> element to "terminated";
 - set the state attribute within the <contact> element to "terminated"; and
 - set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or
 - ii) has been kept registered then:
 - set the state attribute within the <registration> element to "active"; and
 - set the state attribute within the <contact> element to "active"; and
- 5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

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.

In case of the deregistration of the old contact information when the UE is roaming, registration is done in a new network and the previous registration has not expired, on completion of the above procedures, the S-CSCF shall remove the registration information related to the old contact from the local data.

Otherwise, on completion of the above procedures in this subclause for one or more public user identities, the S-CSCF shall deregister those public user identities and the associated implicitly registered public user identities. On completion of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], 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 of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber). On the completion of the Cx Registration-Termination procedure with the HSS, 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 as described in subclause 5.4.1.2.

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 to the saved route information during subscription;
- 2) set the Event header 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 to "shortened"; and
 - f) set the expiry attribute within each <contact> element to an operator defined value; and
- 4) set a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17].

Afterwards the S-CSCF shall wait for the user to reauthenticate (see subclause 5.4.1.2).

NOTE: Network initiated re-authentication may 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 a P-Access-Network-Info header (as received in the REGISTER request from the UE) in the 3rd-party REGISTER 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. The S-CSCF shall not include a P-Access-Network-Info header 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, which shall contain the S-CSCF's SIP URI;
- c) the To header, 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: 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, which shall contain the S-CSCF's SIP URI;
- e) for initial registration and user-initiated reregistration (subclause 5.4.1.2), the Expires header, which shall contain the same value that the S-CSCF returned in the 200 (OK) response for the REGISTER request received form the UE:
- f) for user-initiated deregistration (subclause 5.4.1.4) and network-initiated deregistration (subclause 5.4.1.5), the Expires header, 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, such as IMSI to be delivered to IM SSF). If there is a service information XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [14]), then the S-CSCF shall include it in the message body of the REGISTER request within the <service-info> XML element which is a child XML element of an <ims-3gpp> element with the "version" attribute set to "1" as described in subclause 7.6. For the messages including the 3GPP IMS XML body, the S-CSCF shall set the value of the Content-Type header to include the MIME type specified in subclause 7.6;
- h) for initial registration and user-initiated reregistration, the P-Charging-Vector header, which shall contain the same icid parameter that the S-CSCF received in the original REGISTER request from the UE;
- i) for initial registration and user-initiated reregistration, a P-Charging-Function-Addresses header, which shall contain the values received from the HSS if the message is forwarded within the S-CSCF home network.

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 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 (i.e. the P-CSCF to which this user is attached to); and
 - all the ASs listed in the initial filter criteria and not belonging to third-party providers.

NOTE: The S-CSCF finds the identity of the originator of the SUBSCRIBE request in the P-Asserted-Identity header.

- 2) 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, set to either the same or a decreased value as the Expires header in SUBSCRIBE request;
 and
 - a Contact header, set to is an identifier generated within the S-CSCF that will help to correlate refreshes for the SUBSCRIBE.

Afterwards the S-CSCF shall perform the procedures for notification about registration state as described in subclause 5.4.2.1.2.

5.4.2.1.2 Notification about registration state

For each NOTIFY request 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 to the saved route information during subscription;
- 2) set the Event header 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 the <contact> sub-element of each <registration> element to the contact address provided by the UE; and
 - b) if the public user identity:
 - I) has been deregistered then:
 - set the state attribute within the <registration> element to "terminated";
 - set the state attribute within the <contact> element to "terminated"; and
 - set the event attribute within the <contact> element to "deactivated", "expired", "unregistered", "rejected" or "probation" according RFC 3680 [43]; or
 - II) has been registered then:
 - 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 "registered"; or

III) has been automatically registered:

- 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
- 5) set the P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17].

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

EXAMPLE: 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:

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 to the value of "terminated".

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

5.4.3 General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF

5.4.3.1 Determination of mobile-originated or mobile-terminated case

Upon receipt of an initial request or a target refresh request or a stand-alone transaction, the S-CSCF shall:

- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the request makes use of the information for mobile-originating calls, which was added to the Service-Route header 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 contains a specific user part or parameter; or,
- perform the procedures for the mobile-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

When the S-CSCF receives from the served user an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

- 1) determine whether the request contains a barred public user identity in the P-Asserted-Identity header field of the request or not. In case the said header field contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. Otherwise, continue with the rest of the steps;
- NOTE 1: 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.
- 2) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request;
- 3) remove its own SIP URI from the topmost Route header;
- 4) check whether the initial request matches the next unexecuted initial filter criteria based on a public user identity in the P-Asserted-Identity header in the priority order as described in 3GPP TS 23.218 [5], and if it does, the S-CSCF shall:
 - a) insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4; and
 - b) if the AS is located outside the trust domain then the S-CSCF shall remove the P-Access-Network-Info header field and its values and the access-network-charging-info parameter in the P-Charging-Vector header from the request; if the AS is located within the trust domain, then the S-CSCF shall retain the P-Access-Network-Info header field and its values and the access-network-charging-info parameter in the P-Charging-Vector header in the request that is forwarded to the AS;

- NOTE 2: 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.
- 5) if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. Optionally, the S-CSCF may generate a new, globally unique icid and insert the new value in the icid parameter of the P-Charging-Vector header 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;
- 6) if there is no original dialog identifier present in the topmost Route header of the incoming request insert an originio parameter into the P-Charging-Vector header. The S-CSCF shall set the originio parameter to a value that identifies the sending network. The S-CSCF shall not include the term-ioi parameter;
- 7) if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;
- 8) if there is no original dialog identifier present in the topmost Route header of the incoming request and if in the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URI contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;
- 9) if the request is not forwarded to an AS and if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [22]) to a globally routeable SIP URI using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [24]. Databases aspects of ENUM are outside the scope of the present document. 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. If the request is forwarded, the S-CSCF shall remove the access-network-charging-info parameter from the P-Charging-Vector header prior to forwarding the message;
- 10) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header if present, otherwise based on the Request-URI;
- 11) if network hiding is needed due to local policy, put the address of the I-CSCF(THIG) to the topmost route header;
- 12) in case of an initial request for a dialog the S-CSCF shall create a Record-Route header containing its own SIP URI;
- 13)if the destination user (Request-URI) lies outside of the trust domain of the S-CSCF, remove the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header, prior to forwarding the message;
- 14) route the request based on SIP routeing procedures; and
- 15) 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 any response to the above request, the S-CSCF may:

- 1) apply any privacy required by RFC 3323 [33] to the P-Asserted-Identity header.
- NOTE 3: This header would normally only be expected in 1xx or 2xx responses.
- NOTE 4: 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 3323 [33].

When the S-CSCF receives any response to the above request containing a term-ioi parameter, the S-CSCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present. The term-ioi parameter identifies the sending network of the response message. The term-ioi parameter and the orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS.

When the S-CSCF receives a 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 from the served user 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;
- 2) create a Record-Route header containing its own SIP URI;
- 3) 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;
- 4) in case the request is routed towards the destination user (Request-URI)or is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header; and
- 5) route the request based on the topmost Route header.

When the S-CSCF receives a 1xx or 2xx response to the target refresh 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 such that the S-CSCF is able to release the session if needed.

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;
- 2) in case the request is routed towards the destination user (Request-URI)or is routed to an AS located outside the trust domain, remove the P-access-network-info header and the access-network-charging-info parameter in the P-Charging-Vector header; and
- 3) route the request based on the topmost Route header.

5.4.3.3 Requests terminated at the served user

When the S-CSCF receives, destined for a registered served user, an initial request for a dialog or a request for a standalone transaction, 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 is present in the topmost Route header of the incoming request.
 - If present, it indicates an association with an existing dialog, 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 whether the request contains a barred public user identity in the Request-URI of the request or not. In case the Request URI contains 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 and continue with the rest of the steps;
- 2) remove its own URI from the topmost Route header;
- 3) if there was an original dialog identifier present in the topmost Route header of the incoming request check whether the Request-URI equals to the saved value of the Request-URI. If there is no match, then:
 - a) 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; and
 - b) forward the request based on the topmost Route header or if not available forward the request based on the Request-URI (routing based on Request-URI is specified in steps 10 through 14 from subclause 5.4.3.2) and skip the following steps;
- 4) check whether the initial request matches the next unexecuted initial filter criteria 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 insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

- NOTE 1: Depending on the result of the previous process, the S-CSCF may contact one or more AS(s) before processing the outgoing Request-URI.
- 5) if there was no original dialog identifier present in the topmost Route header 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 of the incoming request store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header;
- 7) if there was no original dialog identifier present in the topmost Route header of the incoming store the value of the orig-ioi parameter received in the P-Charging-Vector header, if present. The orig-ioi parameter identifies the sending network of the request message. The orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS;
- 8) in case there are no Route headers in the request, then determine, from the destination public user identity, the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2. Furthermore, the S-CSCF shall:
 - a) build the Route header field with the values determined in the previous step;
 - b) determine, from the destination public user identity, the saved Contact URI where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2;
 - c) build a Request-URI with the contents of the saved Contact URI determined in the previous step; and
 - d) insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;
- 9) 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;
- 10) optionally, apply any privacy required by RFC 3323 [33] to the P-Asserted-Identity header; and
- NOTE 2: 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 3323 [33].
- 11) forward the request based on the topmost Route header.

When the S-CSCF receives, destined for an unregistered user, an initial request for a dialog or a request for a standalone transaction, the S-CSCF shall:

- 1) if the S-CSCF does not have the user profile, then initiate the S-CSCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informing the HSS that the user is unregistered, but this S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14];
- 2) execute the procedures described in the steps 1, 2 and 3 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); and
- 3) execute the procedure described in step 4, 5, 6, 7, 8, 9, 11 and 12 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).

In case that no 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.

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), it 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) insert an term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi;
- 3) in the case where the S-CSCF has knowledge of an associated tel-URL for a SIP URI contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel-URL; and
- 4) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header.

When the S-CSCF receives a response to a request for a standalone transaction (whether the user is registered or not), in the case where the S-CSCF has knowledge of an associated tel-URL for a SIP URI contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel-URL. In case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header.

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 populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards an AS; and
- 2) insert a term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi.

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:

- 1) remove its own URI from the topmost Route header;
- 2) 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;
- 3) create a Record-Route header containing its own SIP URI; and
- 4) forward the request based on the topmost Route header.

When the S-CSCF receives a 1xx or 2xx response to the target refresh 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 Record-Route and 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 P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header.

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) remove its own URI from the topmost Route header; and
- 2) forward the request based on the topmost Route header.

When the S-CSCF receives a response to a 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 P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header.

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, 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 identifies 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. 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 and make the proper association between related dialogs that pass through an AS.

5.4.3.5 Void

5.4.4 Call initiation

5.4.4.1 Initial INVITE

Void.

5.4.4.2 Subsequent requests

5.4.4.2.1 Mobile-originating case

When the S-CSCF receives any 1xx or 2xx response, the S-CSCF shall insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

When the S-CSCF receives the UPDATE request, the S-CSCF shall store the access-network-charging-info parameter from the P-Charging-Vector header. The S-CSCF shall retain access-network-charging-info parameter in the P-Charging-Vector header 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 when the UPDATE 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 mobile-originated dialog or standalone transaction, the S-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message within the S-CSCF home network, including towards AS.

5.4.4.2.2 Mobile-terminating case

When the S-CSCF receives the any 1xx or 2xx response, the S-CSCF shall insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

When the S-CSCF receives 180 (Ringing) or 200 (OK) (to INVITE) responses, the S-CSCF shall store the access-network-charging-info parameter from the P-Charging-Vector header. The S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header 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 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 mobile-terminated dialog or standalone transaction, the S-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message within the S-CSCF home network, including towards AS.

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 an network internal indication to release a session which is currently being established, the S-CSCF shall cancel the related dialogs by sending the CANCEL request according to the procedures described in RFC 3261 [26].

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) generate a first BYE request for the called user based on the information saved for the related dialog, including:
 - a Request-URI, set to the stored Contact header provided by the called user;
 - 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 routeing information towards the called user as stored for the dialog;
 - further headers, based on local policy or the requested session release reason.
- 2) generate a second BYE request for the calling user based on the information saved for the related dialog, including:
 - a Request-URI, set to the stored Contact header provided by the calling user;
 - a To header, set to the From header value as received in the initial INVITE request;
 - a From header, set to the To header value as received in the 200 OK response for 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 called to the calling user, incremented by one if no CSeq value was stored for that session it shall generate and apply a random number within the valid range for CSeqs;
 - a Route header, set to the routeing information towards the calling user as stored for the dialog;
 - further headers, based on local policy or the requested session release reason.
- 3) if the S-CSCF serves the calling user, treat the first BYE request as if received directly from the calling user, i.e. send it to internal service control and based on the outcome further on towards the called user;
- 4) if the S-CSCF serves the calling user, send the second BYE request directly to the calling user.
- 5) if the S-CSCF serves the called user, send the first BYE request directly to the called user;
- 6) if the S-CSCF serves the called user, treat the second BYE request as if received directly from the called user, i.e. shall send it to internal service control and based on the outcome further on towards to 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 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) expires while there are still active multimedia sessions that includes this user, where the session was initiated with the public user identity currently registered or with one of the implicitly registered public used identities, the S-CSCF shall release each of these multimedia sessions by applying the steps listed in the subclause 5.4.5.1.2.

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.

5.4.6 Call-related requests

5.4.6.1 ReINVITE

5.4.6.1.1 Determination of served user

Void.

5.4.6.1.2 Mobile-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 in the received SIP request. The S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header 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 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 P-Access-Network-Info header and the access-network-charging-info parameter from the P-Charging-Vector header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter from the P-Charging-Vector header.

5.4.6.1.3 Mobile-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. The S-CSCF shall retain the access-network-charging-info parameter in the P-Charging-Vector header when the response is forwarded to the AS. However, the S-CSCF shall include the access-network-charging-info parameter in the P-Charging-Vector header 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 P-Access-Network-Info header and the access-network-charging-info parameter from the P-Charging-Vector header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter from the P-Charging-Vector header.

5.4.7 Void

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 headers shall not be supported by the MGCF.

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 headers before sending the message.

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:

- generate and send an INVITE request to I-CSCF:
 - set the Request-URI to the "tel" format using an E.164 address;
 - set the Supported header to "100rel" (see RFC 3312 [30]);
 - include an P-Asserted-Identity header;
 - create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and
 - insert an orig-ioi parameter into the P-Charging-Vector header. The orig-ioi parameter shall be set to a value that identifies the sending network in which the MGCF resides and the term-ioi 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 parameter received in the P-Charging-Vector header, if present. The term-ioi parameter identifies the sending network of the response message.

5.5.3.1.2 Calls terminating in circuit-switched networks

When the MGCF receives an initial INVITE request with Supported header indicating "100rel", the MGCF shall:

- store the value of the orig-ioi parameter received in the P-Charging-Vector header, if present. The orig-ioi parameter identifies the sending network of the request message.
- send 100 (Trying) response;
- after a matching codec is found at the MGW, send 183 "Session Progress" response:
 - set the Require header to the value of "100rel";
 - store the values received in the P-Charging-Function-Addresses header;

- store the value of the icid parameter received in the P-Charging-Vector header; and
- insert a term-ioi parameter into the P-Charging-Vector header. The term-ioi parameter shall be set to a value that identifies the network in which the MGCF resides.

When 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.

5.5.3.2 Subsequent requests

5.5.3.2.1 Calls originating in circuit-switched networks

When the MGCF receives 183 response to an INVITE request, the MGCF shall:

- store the values received in the P-Charging-Function-Addresses header.

When the MGCF receives 200 (OK) response to a PRACK request and notification that bearer setup is complete, the MGCF shall:

- send an UPDATE 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 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 to the UE, including an P-Asserted-Identity header.

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 signaling 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 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 may be used in the interim.

5.6 Procedures at the BGCF

5.6.1 General

The use of the Path and Service-Route headers shall not be supported by the BGCF.

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 headers before forwarding the message.

5.6.2 Session initiation transaction

When the BGCF receives an INVITE request, the BGCF shall forward the request either to an MGCF within its own network, or to another network containing an MGCF. The BGCF need not Record-Route the INVITE request. 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. The BGCF shall store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header.

NOTE: 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 may be by means of a lookup to an external database, or may be by data held internally to the BGCF.

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 containing information about the user's registration status and the AS supports the REGISTER method, the AS shall store the Expires parameter from the request and generate a 200 (OK) response or an appropriate failure response. For the success case, the 200 (OK) response shall contain Expires value equal to the value received in the

REGISTER request. The AS shall store the values received in P-Charging-Function-Addresses header. Also, the AS shall store the values of the icid parameter in the P-Charging-Vector header from the REGISTER request.

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 users 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 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 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 with the icid parameter populated as specified in 3GPP TS 32.225 [17].

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 of the received response.

NOTE 2: 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 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 containing a value of zero.

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, e.g. icid parameter, and retain the P-Charging-Vector header in the message. The AS shall store the values received in the P-Charging-Function-Addresses header 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 headers before sending the message.

5.7.1.3 Access-Network-Info

The AS may receive in any request or response (excluding ACK requests and CANCEL requests and responses) information about the served user access network. This information is contained in the P-Access-Network-Info header. The AS can use the header to provide an appropriate service to the user.

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.

An AS acting as redirect server shall propagate any received 3GPP 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 with the icid parameter populated as specified in 3GPP TS 32.225 [17].

5.7.3 Application Server (AS) acting as originating UA

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. 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 with the icid parameter populated as specified in 3GPP TS 32.225 [17]. The AS may retrieve CCF and/or ECF adresses from HSS on Sh interface.

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 with the icid parameter populated as specified in 3GPP TS 32.225 [17].

The AS shall extract charging function addresses from any P-Charging-Function-Addresses header that is received in any 1xx or 2xx responses to the requests.

Furthermore the AS shall insert a Route header pointing to the S-CSCF of the UE on whose behalf the request is generated.

NOTE: The address of the S-CSCF may be obtained either from a previous request terminated by the AS, by querying the HSS on the Sh interface or from static configuration.

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 it shall:

- remove its own URI from the topmost Route header; and
- after executing the required services, route the request based on the topmost Route header.

The AS may modify the SIP requests based on service logic, prior to forwarding the request back to the S-CSCF.

An AS acting as a SIP proxy shall propagate any received 3GPP message body in the forwarded message.

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:

- Routeing B2BUA: an AS receives a request from S-CSCF, 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.

The B2BUA AS will internally map the message headers 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 S-CSCF shall copy the remaining Route header(s) unchanged from the received request for a standalone transaction to the new request for a standalone transaction.

5.7.5.2 Call initiation

5.7.5.2.1 Initial INVITE

When the AS acting as a Routeing B2BUA receives an initial INVITE request from the S-CSCF, the AS shall:

- remove its own SIP URI from the topmost Route header of the received INVITE request;
- perform the AS specific functions. See 3GPP TS 23.218 [5];
- if successful, generate and send a new INVITE request to the S-CSCF to establish a new dialog;
- copy the remaining Route header(s) unchanged from the received INVITE request to the new INVITE request;
- route the new INVITE request based on the topmost Route header.

NOTE: The topmost Route header of the received INVITE request will contain the AS's SIP URI. The following Route header will contain the SIP URI of the S-CSCF.

When the AS is acting as an Initiating B2BUA, the AS shall apply the procedures described in subclause 5.7.3 for both requests. The AS shall either set the icid parameter in the P-Charging-Vector header to be the same as received or different. The AS may retrieve CCF and/or ECF adresses 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 acting as an Initiating B2BUA the AS shall apply the procedures described in subclause 5.7.3 for both requests. The AS shall either set the icid parameter in the P-Charging-Vector header to be the same as received or different.

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.

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 headers before sending the message.

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 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, e.g. icid parameter. The MRFC shall store the values received in the P-Charging-Function-Addresses header.

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 with an indicator for a tone or announcement, the MRFC shall:

- send 100 (Trying) response.

NOTE: The detailed interfaces for requesting tones and announcements are not specified in this version of the document. Other solutions may be used in the interim.

5.8.2.1.1.3 Ad-hoc conferences

The MRFC can receive INVITE requests to set up an ad-hoc conferencing session (e.g. Multiparty Call) or to add parties from the conference. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator to initiate ad hoc conferencing, the MRFC shall:

- send 100 (Trying) response; and
- after the MRFP indicates that the conference resources are available, send 200 (OK) response with an MRFC conference identifier. If the MRFC chooses to send a 183 (Session Progress) response prior to the 200 (OK), then the conference identifier may also be included in the 183 (Session Progress) response.

When the MRFC receives an INVITE request with an indicator to add a party to an existing ad hoc conference (i.e. MRFC conference identifier), the MRFC shall:

- send 100 Trying response; and
- after the MRFP indicates that the conferencing request is granted, send 200 OK response with the MRFC conference identifier. If the MRFC chooses to send a 183 Session Progress response prior to the 200 OK, then the conference identifier may also be included in the 183 Session Progress response.

NOTE: The detailed interface for requesting ad-hoc conferencing sessions is not specified in this version of the document. Other solutions may be used in the interim.

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 with an indicator for transcoding and a codec is supplied in SDP, the MRFC shall:

- send 100 (Trying) response; and

- after the MRFP indicates that the transcoding request is granted, send 200 (OK) 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 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 with the icid parameter populated as specified in 3GPP TS 32.225 [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.

5.8.3 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.

5.8.2.2.2 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.

5.8.4 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 (e.g. 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 with the MRFC conference identifier. If the MRFC chooses to send a 183 (Session Progress) response prior to the 200 OK, then the conference identifier may also be included in the 183 (Session Progress) response.

NOTE: The detailed interface for requesting ad-hoc conferencing sessions is not specified in this version of the document. Other solutions may be used in the interim.

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: The detailed interface for requesting MRFC/MRFP capabilities is not specified in this version of the document. Other solutions may be used in the interim.

6 Application usage of SDP

6.1 Procedures at the UE

Usage of SDP by the UE:

- 1. In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.
- 2. An INVITE request generated by a UE shall contain SDP payload. The SDP payload shall reflect the calling user's terminal capabilities and user preferences for the session. The UE shall order the codecs with the most preferred codec listed first. In addition, the calling user shall indicate the desired QoS for the session, using the segmented status type. In an initial INVITE request the UE shall indicate that it mandates local QoS and that this precondition is not yet satisfied, i.e. or the local segment the UE shall include the following preconditions:
 - a) a desired-status attribute line set in accordance with RFC 3312 [30] in the following manner:
 - the precondition-type attribute set to "qos";
 - the strength attribute attribute set to "mandatory";
 - the status-type attribute set to "local"; and
 - the direction-tag attribute in accordance with the direction of the related media stream; and
 - b) a current-status attribute line set in accordance with RFC 3312 [30] in the following manner:
 - the precondition-type attribute set to "qos";
 - the status-type attribute set to "local"; and
 - the direction-tag attribute set to "none".
- 3. Providing that the INVITE request received by the UE contains an SDP offer including one or more "m=" media descriptions, the first 183 (Session Progress) provisional response that the UE sends, shall contain the answer for the SDP received in the INVITE. The said SDP answer shall reflect the called user's terminal capabilities and user preferences.
- 4. When the UE sends a 183 (Session Progress) response with SDP payload including one or more "m=" media descriptions, it shall request confirmation for the result of the resource reservation at the originating end point.
- 5. During session establishment procedure, and during session modification procedures, SIP messages shall only contain SDP payload 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.

6. 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.

If the media line in the SDP indicates the usage of RTP/RTCP, 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.

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 3GPP TS 29.208 [13].

- NOTE 2: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifer will typically get the value of zero.
- 7. 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 types associated with the audio codecs for the media stream, the MIME

- subtype "telephone-event" in the SDP "m=" media descriptor associated with the media stream, to indicate support of in-band DTMF as described in RFC 2833 [23].
- 8. The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 [54] and perform the action outlined in subclause 9.2.5.
- 9. If a PDP context is rejected or modified, the UE shall, if the SDP is affected, update the remote SIP entity according to RFC 3261 [26] and RFC 3311 [29].
- 10. If the UE builds SDP for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to 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 payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) responses.
- NOTE 3: The UE may be attempting a session establishment through multiple networks with different policies and potentially may 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 contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

6.2 Procedures at the P-CSCF

When the P-CSCF receives any SIP request containing SDP, the P-CSCF shall examine the media parameters in the received SDP. If the P-CSCF finds any media parameters which are not allowed on the network by local policy, the P-CSCF shall return a 488 (Not Acceptable Here) response containing SDP payload. This SDP payload 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. The P-CSCF shall build the SDP payload in the 488 (Not Acceptable Here) response in the same manner as a UAS builds the SDP in a 488 (Not Acceptable Here) response as specifed in RFC 3261 [26]. For each media line, the P-CSCF shall order the codecs with the most preferred codec listed first.

When the P-CSCF receives an initial INVITE request for a terminating session setup or a 183 (Session Progress) response to an INVITE request for an originating session setup, the P-CSCF may modify the SDP according to RFC 3524 [54] to indicate to the UE that particular media stream(s) is grouped according to a local policy. The policy is used to determine whether the P-CSCF will request the UE to keep media stream(s) grouped in different PDP contexts and identify the relation between different media streams and PDP contexts (see subclause 9.2.5).

The P-CSCF shall apply and maintain the same policy within the SDP from the initial request or response containing SDP and throughout the complete SIP session. If a media stream is added and grouping apply to the session, the P-CSCF shall modify the SDP according to RFC 3524 [54] to indicate to the UE that the added media stream(s) will be grouped into either a new group or into one of the existing groups. The P-CSCF shall not indicate re-grouping of media stream(s) within the SDP.

The P-CSCF shall not apply RFC 3524 [54] to the SDP for additional media stream(s), if grouping of media stream(s) was not indicated in the initial INVITE request or 183 (Session Progress) response.

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.

6.3 Procedures at the S-CSCF

When the S-CSCF receives any SIP request containing SDP, the S-CSCF shall examine the media parameters in the received SDP. If the S-CSCF finds any media parameters which are not allowed based on either local policy or the subscription, the S-CSCF shall return a 488 (Not Acceptable Here) response containing SDP payload. This SDP payload 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 payload in the 488 (Not Acceptable Here) response in the same manner as a UAS builds the SDP in a 488 (Not Acceptable Here) response as specified in RFC 3261 [26].

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 exception:

- In an INVITE request generated by a MGCF, the MGCF shall indicate the current status of the precondition.

When sending an SDP, the MGCF shall not include the "i=", "u=", "e=", "p=", "r=", and "z=" descriptors in the SDP, and it shall ignore them when received in the SDP.

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 (see 3GPP TS 26.235 [10] for the supported codecs); and
- in order to support DTMF, populate the SDP with MIME subtype "telephone-event" as described in RFC 2833 [23].

When the MGCF receives 183 (Session Progress) response to an INVITE request, the MGCF shall:

- check that a supported codec has been indicated in the SDP.

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 exception:

When the MGCF sends a 183 (Session Progress) response with SDP payload, it shall only request confirmation
for the result of the resource reservation at the originating end point if there are any remaining unfulfilled
preconditions.

When sending an SDP, the MGCF shall not include the "i=", "u=", "e=", "p=", "r=", and "z=" descriptors in the SDP, and it shall ignore them when received in the SDP.

When the MGCF receives an initial INVITE request, the MGCF shall:

- check for a codec that matches the requested SDP, which may include the MIME subtype "telephone-event" as described in RFC 2833 [23].

When the MGCF generates and sends a 183 (Session Progress) response to an initial INVITE request, the MGCF shall:

- set SDP indicating the selected codec, which may include the MIME subtype "telephone-event" as described in RFC 2833 [23].

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:

Providing that an INVITE request generated by an AS contains SDP payload, the AS has the capability of
reflecting the originating AS's capabilities, desired QoS and precondition requirements for the session in the SDP
payload.

2) When the AS sends a 183 (Session Progress) response with SDP payload 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.

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 headers defined within the present document

7.2.0 General

There are no SIP headers defined within the present document over and above those defined in the referenced IETF specifications.

7.2.1	Void

7.2.2	Void
1 / /	VOICE
1	v Ola

7.2.9 Void

7.2.10 Void

7.2A Extensions to SIP headers defined within the present document

7.2A.1 Extension to WWW-authenticate header

7.2A.1.1 Introduction

This extension defines a new authentication parameter (auth-param) for the WWW-Authenticate header 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 7.4.

Table 7.4: 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 = LDQUOT *(HEXDIG) RDQUOT
ck-value = LDQUOT *(HEXDIG) RDQUOT
```

7.2A.1.3 Operation

This authentication parameter will be used in a 401 (Unauthorized) response in the WWW-authenticate header 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 in a 401 (Unauthorized) response. The P-CSCF stores the integrity-key value and removes the integrity-key parameter from the header prior to forwarding the response to the UE.

The S-CSCF appends the cipher-key parameter (directive) to the WWW-Authenticate header in a 401 (Unauthorized) response. The P-CSCF removes the cipher-key parameter from the header 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

7.2A.2.1 Introduction

This extension defines a new auth-param for the Authorization header 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 is specified in table 7.5.

Table 7.5: Syntax of auth-param for Authorization header

```
auth-param = "integrity-protected" EQUAL ("yes" / "no")
```

7.2A.2.3 Operation

This authentication parameter is inserted by the P-CSCF in the Authorization header of all the REGISTER requests received from the UE. The value of the "integrity protected" field 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.

7.2A.3 Tokenized-by parameter definition (various headers)

7.2A.3.1 Introduction

The tokenized-by parameter is an extension parameter appended to encrypted entries in various SIP headers as defined in subclause 5.3.3.1.

7.2A.3.2 Syntax

The syntax for the tokenized-by parameter is specified in table 7.6:

Table 7.6: Syntax of tokenized-by-param

The BNF for uri-parameter is taken from IETF RFC 3261 [26] and modified accordingly.

7.2A.3.3 Operation

The tokenized-by parameter is appended by I-CSCF(THIG) after all encrypted strings within SIP headers when network configuration hiding is active. The value of the parameter is the domain name of the network which encrypts the information.

7.2A.4 P-Access-Network-Info header

7.2A.4.1 Introduction

The P-Access-Network-Info header is extended to include specific information relating to 3GPP access networks.

7.2A.4.2 Syntax

The syntax of the P-Access-Network-Info header is described in RFC 3455 [52].

7.2A.4.3 Additional coding rules for P-Access-Network-Info header

In 3GPP systems, there are additional coding rules for the P-Access-Network-Info header:

If the *access type* field is equal to "3GPP-GERAN" the *access info* field shall contain a value for "cgi-3gpp" parameter. This value shall be 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).

If the *access type* field is equal to "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD" or "3GPP-CDMA2000" the *access info* field shall contain a value for "utran-cell-id-3gpp" parameter. This value shall be made up of 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).

7.2A.5 P-Charging-Vector header

7.2A.5.1 Introduction

The P-Charging-Vector header is is extended to include specific charging correlation information needed for IM CN subsystem functional entities.

7.2A.5.2 Syntax

The P-Charging-Vector header field has the syntax described in RFC 3455 [52]. Table 7.3 describes extensions required for 3GPP to that syntax.

Table 7.3: Syntax of extensions to P-Charging-Vector header

```
access-network-charging-info = (gprs-charging-info / 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]
```

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header.

The access-network-charging-info parameter includes alternative definitions for different types access networks.

GPRS is the initially 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 parameters that contains the information for one or more PDP contexts. 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. 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 flow 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 29.207 [12] Annex C. The gcid and flow-id parameters are transferred from the GGSN to the P-CSCF (PDF) over the Go interface, see 3GPP TS 29.207 [12].

The gcid value is received in binary format at the P-CSCF (see 3GPP TS 29.207 [12]). The P-CSCF shall encode it in hexadecimal format before including it into the gcid parameter. On receipt of this header, a node receiving a gcid shall decode from hexadecimal into binary format.

For a dedicated PDP context for SIP signalling, i.e. no media stream requested for a session, then there is no authorisation activity or information exchange over the Go interface. Since there are no GCID, media authorization token or flow identifiers in this case, the GCID and media authorization token are set to zero and no flow identifier parameters are constructed by the P-CSCF/PDF.

7.2A.5.3 Operation

The operation of this header is described in subclauses 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8.

7.2A.6 Void

7.2A.7 Extension to Security-Client, Security-Server and Security-Verify headers

7.2A.7.1 Introduction

This extension defines new paramerts for the Security-Client, Security-Server and Security-Verify headers.

7.2A.7.2 Syntax

The syntax for the Security-Client, Security-Server and Security-Verify headers is defined in IETF RFC 3329. The additional syntax is defined in Annex H of 3GPP TS 33.203 [19].

7.2A.7.3 Operation

The operation of the additional parameters for the Security-Client, Security-Server and Security-Verify headers is defined in Annex H of 3GPP TS 33.203 [19].

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

There are no session description types defined within the present document over and above those defined in the referenced IETF specifications.

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 7.7A.

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.

The associated MIME type with the 3GPP IMS XML body is "application/3gpp-ims+xml".

7.6.2 Document Type Definition

The XML Schema is defined in table 7.7A.

Table 7.7A: 3GPP 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"</pre>
       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 name="type" type="xs:string"/>
     <xs:element name="reason" type="xs:string"/>
      <xs:any namespace="##any" processContents="lax" minOccurs="0" maxOccurs="unbounded"/>
   </xs:sequence>
   <xs:anvAttribute/>
</xs:complexType>
<xs:element name="ims-3gpp" type="tIMS3GPP"/>
```

7.6.3 XML Schema description

This subclause describes the elements of the 3GPP IMS Document Type Definition as defined in table 7.7A.

<ims-3gpp>:

This is the root element of the 3GPP IMS XML body. It shall always be present. XML instance documents of future versions of the XML Schema in table 7.7A shall be valid against the XML Schema in table 7.7A in this document. XML instance documents of the XML Schema in table 7.7A in the present document shall 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. 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.

> The <alternative-service> element contains a <type> element that indicates the type of alternative service. In the present document, the <type> element contains only the value specified in table 7.7AA.

Table 7.7AA: ABNF syntax of value of the <type> element

```
emergency-value = %x65.6D.65.72.67.65.6E.63.79; "emergency".
```

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.

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 7.8 shows recommended values for 3GPP.

Table 7.8 lists in the first column, titled "SIP Timer" the timer names as defined in RFC 3261 [26].

The second column, titled "3GPP value to be applied between network 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 "3GPP value to be applied at the UE" lists the values recommended for the UE. These are modified when compared to RFC 3261 [26] to accommodate the air interface delays.

The fourth column, titled "3GPP 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. These are modified when compared to RFC 3261 [26].

The final column reflects the timer meaning as defined in RFC 3261 [26].

Table 7.8: SIP timers

SIP Timer	3GPP value to be applied between network elements	3GPP value to be applied at the UE	3GPP value to be applied at the P-CSCF toward a UE	Meaning
T1	500ms default	2s default	2s default	RTT estimate
T2	4s	16s	16s	The maximum retransmit interval for non-INVITE requests and INVITE responses
T4	5s	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	>128s	>128s	Wait time for response retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
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	T4 for UDP	T4 for UDP	Wait time for ACK retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
Timer J	64*T1 for UDP	64*T1 for UDP	64*T1 for UDP	Wait time for non-INVITE request
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	retransmits
Timer K	T4 for UDP	T4 for UDP	T4 for UDP	Wait time for response retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	

7.8 IM CN subsystem timers

Table 7.9 shows recommended values for timers specific to the IM CN subsystem.

Table 7.9: 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		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.
				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.

8 SIP compression

8.1 SIP compression procedures at the UE

8.1.1 SIP compression

The UE shall support SigComp as specified in RFC 3320 [32]. When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486 [55]. The compartment shall finish when the UE is no longer registered. State creations and announcements shall be allowed only for messages received in a security association.

The UE shall support the SIP dictionary specified in RFC 3485 [42]. If compression is enabled, the UE shall use the dictionary to compress the first message.

8.1.2 Compression of SIP requests and responses transmitted to the P-CSCF

The UE should compress the requests and responses transmitted to the P-CSCF according to subclause 8.1.1.

NOTE: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

8.1.3 Decompression of SIP requests and responses received from the P-CSCF

The UE shall decompress the compressed requests and responses received from the P-CSCF according to subclause 8.1.1.

If the UE detects a decompression failure at the P-CSCF, the recovery mechanism is implementation specific and this may, as an example, include resetting the compartment, changing the algorithm or sending the following message(s) without compression.

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]. When using SigComp the P-CSCF shall send compressed SIP messages in accordance with RFC 3486 [55]. The compartment shall finish when the UE is no longer registered. State creations and announcements shall be allowed only for messages received in a security association.

The P-CSCF shall support the SIP dictionary specified in RFC 3485 [42]. If compression is enabled, the P-CSCF shall use the dictionary to compress the first message.

8.2.2 Compression of SIP requests and responses transmitted to the UE

The P-CSCF should compress the requests and responses transmitted to the UE according to subclause 8.2.1.

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 and this may, as an example, include resetting the compartment, changing the algorithm or sending the following message(s) without compression.

9 GPRS aspects when connected to the IM CN subsystem

9.1 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] and 3GPP TS 29.207 [12].

9.2 Procedures at the UE

9.2.1 PDP context activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

- a) perform a GPRS attach procedure;
- b) establish 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]. 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 IPv6 address;

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 IE;

II. A general-purpose PDP context:

The UE may decide to use a general-purpose PDP Context to carry IM CN subsystem-related signaling. 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 IE.

The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE 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 IE. 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 IE 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 IE are described in 3GPP TS 24.008 [8].

NOTE: A general-purpose PDP Context may carry both IM CN subsystem signaling and media, in case the media does not need to be authorized by 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. Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and the DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] after PDP context activation.

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 IPv6 addresses of P-CSCF(s).
- 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 IE 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 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 IE as the P-CSCF address with the highest priority.

The UE can freely select method I or II for P-CSCF discovery. 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 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.

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.

The UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options IE when activating a PDP context according to 3GPP TS 27.060 [10A].

The encoding of the request and response for IPv6 address(es) for DNS server(s) and list of P-CSCF address(es) within the Protocol Configuration Options IE is described in 3GPP TS 24.008 [8].

9.2.1A 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 IE 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 IE 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 IE of the MODIFY PDP CONTEXT RESPONSE message.

9.2.1B Re-establishment of the PDP context for signalling

If the dedicated PDP context for SIP signalling is lost due to e.g. a GPRS routeing area update procedure, the UE shall attempt to re-establish the dedicated PDP context for SIP signalling. If this procedure does not succeed, the UE shall deactivate all PDP contexts established as a result of SIP signalling according to the 3GPP TS 24.008 [8].

9.2.2 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.

9.2.3 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.

9.2.4 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.

9.2.5 PDP contexts for media

9.2.5.1 General requirements

The UE shall establish different PDP contexts for media streams that belong to different SIP sessions.

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.

When the UE has to allocate bandwidth for RTP and RTCP in a PDP context, the UE shall use the rules outlined in 3GPP TS 29.208 [13].

9.2.5.1A Activation or modification of PDP contexts for 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. The UE may freely group media streams to PDP context(s) in case no indication of grouping is received from the P-CSCF.

The UE can receive a media authorization token in the P-Media-Authorization header from the P-CSCF according to RFC 3313 [31]. The UE shall, if a media authorization token is received in the P-Media-Authorization header when a SIP session is initiated, establish separate PDP context(s) for the media. 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.

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 IE 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 IE 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].

Detailed description of how the media authorization token and flow identifiers are carried in the Traffic Flow Template IE is provided in 3GPP TS 24.008 [8].

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.

The UE shall not re-use a PDP context for other SIP sessions when the session has an associated media authorization token. The UE shall deactivate the PDP context when the SIP session that provided the media authorization token is terminated. When no media authorization token is used for a SIP session, the UE may reuse the PDP context between different SIP sessions.

The UE shall not include the IM CN Subsystem Signalling Flag when a PDP context for media is established or modified.

9.2.5.2 Special requirements applying to forked responses

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 9.2.5.1A.
- 3) **the subsequent SDP introduces one or more additional IP flows.** The UE establishes additional PDP context(s) according to subclause 9.2.5.1A.
- NOTE 1: 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 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 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 a 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:

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.

9.2.5.3 Unsucessful situations

One of the Go 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 interface related error code, the UE shall either terminate the session or retransmit the message up to three times. The Go interface related error codes are further specified in 3GPP TS 29.207 [12].

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 be 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 parameter after applying procedures such as filtering, insertion of P-Asserted-Identity header, 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 400 (Bad Request) response; and
 - handle unknown header fields and unknown header 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 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, an 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).			
0	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.			
Х	prohibited (excluded)	It is not allowed to use the capability. This is more common for a profile.			
c <integer></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.</integer>			
o. <integer></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.</integer>			
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 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.

A.1.3 Roles

Table A.2: Roles

Item	Roles	Reference	RFC status	Profile status			
1	User agent	[26]	0.1	0.1			
2	Proxy	[26]	0.1	0.1			
o.1:	o.1: It is mandatory to support exactly one of these items.						
NOTE:							

Table A.3: Roles specific to this profile

Item	Roles	Reference	RFC status	Profile status			
1	UE	5.1	n/a	0.1			
2	P-CSCF	5.2	n/a	0.1			
3	I-CSCF	5.3	n/a	0.1			
3A	I-CSCF (THIG)	5.3	n/a	c1			
4	S-CSCF	5.4	n/a	0.1			
5	BGCF	5.6	n/a	0.1			
6	MGCF	5.5	n/a	0.1			
7	AS	5.7	n/a	0.1			
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	0.1			
c1:	IF A.3/3 THEN o ELSE x I-CSCF.						
c2:	IF A.3/7 THEN o.2 ELSE n/a AS.						
o.1:	It is mandatory to support exactly one of thes	se items.					
o.2:	It is mandatory to support at least one of the	se items.					

entirely separate assessment of the tables shall be made for each role.

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

A.2.1 User agent role

A.2.1.1 Introduction

NOTE:

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 Profile definition for the Session Initiation Protocol as used in the present document

A.2.1.2 Major capabilities

Table A.4: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status	
	Capabilities within main protocol				
1	client behaviour for registration?	[26] subclause 10.2	m	c3	
2	registrar?	[26] subclause 10.3	0	c4	
2A	initiating a session?	[26] subclause 13	0	0	
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	0	0	
7	authentication between UA and UA?	[26] subclause 22.2	0	0	
8	authentication between UA and registrar?	[26] subclause 22.2	0	n/a	
8A	authentication between UA and proxy?	[26] 20.28, 22.3	0	0	
9	server handling of merged requests due [26] 8.2.2 to forking?		m	m	
10	client handling of multiple responses [26] 13.2.2.4 due to forking?		m	m	
11	insertion of date in requests and responses?	[26] subclause 20.17	0	0	
12	downloading of alerting information?	[26] subclause 20.4	0	0	
	Extensions				
13 the SIP INFO method?		[25]	0	n/a	
14	reliability of provisional responses in SIP?	[27]	c19	c18	
15	the REFER method?	[36]	0	0	
16	integration of resource management and SIP?	[30]	c19	c18	
17	the SIP UPDATE method?	[29]	c5	c18	
19	SIP extensions for media authorization?	[31]	0	c14	
20	SIP specific event notification?	[28]	0	c13	
21	the use of NOTIFY to establish a dialog?	[28] 4.2	0	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]	0	c6	
25	private extensions to the Session Initiation Protocol (SIP) for network asserted identity within trusted networks?	[34]	0	m	
26	a privacy mechanism for the Session Initiation Protocol (SIP)?	[33]	0	m	
26A	request of privacy by the inclusion of a Privacy header indicating any privacy option?	[33]	с9	c11	
26B	application of privacy based on the received Privacy header?	[33]	с9	n/a	
26C	passing on of the Privacy header transparently?	[33]	с9	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
27	a messaging mechanism for the Session Initiation Protocol (SIP)?	[50]	0	c7
28	session initiation protocol extension header field for service route discovery during registration?	[38]	0	c17
29	compressing the session initiation protocol?	[55]	0	c8
30	private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)?	[52]	0	m
31	the P-Associated-URI header extension?	[52] 4.1	c21	c22
32	the P-Called-Party-ID header extension?	[52] 4.2	c21	c23
33	the P-Visited-Network-ID header extension?	[52] 4.3	c21	c24
34	the P-Access-Network-Info header extension?	[52] 4.4	c21	c25
35	the P-Charging-Function-Addresses header extension?	[52] 4.5	c21	c26
36	the P-Charging-Vector header extension?	[52] 4.6	c21	c26
37	security mechanism agreement for the session initiation protocol?	[48]	0	c20

- 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 THEN m ELSE n/a - UE or S-CSCF functional entity.
- c4: IF A.3/4 OR A.3/7 THEN m 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 THEN m ELSE n/a. - S-CSCF or UE.
- c7: IF A.3/1 OR A.3/4 OR A.3/7A OR A.3/7B OR A.3/7D THEN m ELSE n/a - UA or S-CSCF or AS acting as terminating UA or AS acting as originating UA or AS performing 3rd party call control..
- c8: IF A.3/1 THEN m ELSE n/a - UE behaviour.
- 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 THEN o ELSE n/a - UE or MGCF.
- c12: IF A.3/7D THEN m ELSE n/a - AS performing 3rd-party call control.
- c13: IF A.3/1 OR A.3/4 THEN m ELSE o - UE behaviour or S-CSCF.
- c14: IF A.3/1 THEN m ELSE IF A.3/2 THEN o ELSE n/a UE or P-CSCF.
- c15: IF A.4/20 and A.3/4 THEN m ELSE o SIP specific event notification extensions and S-CSCF.
- c16: IF A.4/20 and (A.3/1 OR A.3/2) THEN m ELSE o - SIP specific event notification extension and UE or P-CSCF.
- c17: IF A.3/1 or A.3/4 THEN m ELSE n/a - UE or S-CSCF.
- c18: IF A.4/2A THEN m ELSE n/a - initiating sessions.
- c19: IF A.4/2A THEN o ELSE n/a - initiating sessions.
- c20: IF A.3/1 THEN m ELSE n/a - UE behaviour.
- c21: IF A.4/30 THEN o.4 ELSE n/a - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP).
- c22: IF A.4/30 AND (A.3/1 OR A.3/4) THEN m ELSE n/a - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF or UA.
- c23: IF A.4/30 AND A.3/1 THEN o ELSE n/a - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE.
- c24: IF A.4/30 AND A.3/4) THEN m ELSE n/a - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF.
- c25: IF A.4/30 AND (A.3/1 OR A.3/4 OR A.3/7A OR A.3/7D) THEN m ELSE n/a - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE, S-CSCF or AS acting as terminating UA or AS acting as third-party call controller.
- c26: IF A.4/30 AND (A.3/6 OR A.3/7A OR A.3/7B or A.3/7D) THEN m ELSE n/a - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and MGCF, AS acting as a terminating UA, or AS acting as an originating UA, or AS acting as third-party call controller.
- c27: IF A.3/7D THEN o ELSE x - AS performing 3rd party call control.
- 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.

A.2.1.3 PDUs

Table A.5: Supported methods

Item	PDU	Sending				Receiving		
		Ref. RFC Profile			Ref.	RFC	Profile	
			status	status		status	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	
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	с7	c7	[50] 7	с7	c7	
9B	MESSAGE response	[50] 4	с7	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	
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	с9	
19	REGISTER response	[26] 10	c9	с9	[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	[30] 6.1	c6	c6	[30] 6.2	c6	c6	
23	UPDATE response	[30] 6.2	c6	c6	[30] 6.1	c6	c6	
c1:	IF A.4/15 THEN m ELSE n/a	the REFER r	method exter	sion.				
c3:	IF A.4/23 THEN m ELSE n/a	recipient for	event informa	ation.				
c4:	IF A.4/22 THEN m ELSE n/a							
c5:	IF A.4/14 THEN m ELSE n/a				ension.			
c6:	IF A.4/17 THEN m ELSE n/a							
c7:	IF A.4/27 THEN m ELSE n/a							
c8:	IF A.4/1 THEN m ELSE n/a o	lient behavio	ur for registra	ation.				
c9:	IF A.4/2 THEN m ELSE n/a r	egistrar.						
c10:	IF A.4/3 THEN m ELSE n/a o							
c11:	IF A.4/4 THEN m ELSE n/a s			E requests.				
c12:	IF A.4/5 THEN m ELSE n/a s	ession releas	se.					

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	Profile		RFC	Profile	
			status	status		status	status	
1	100 (Trying)	[26] 21.1.1	n/a	n/a	[26] 21.1.1	m	m	
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	c1	c1	[26] 21.1.5	c1	c1	
6	200 (OK)	[26] 21.2.1			[26] 21.2.1			
7	202 (Accepted)	[28] 8.3.1	с3	c3	[28] 8.3.1	с3	c3	
8	300 (Multiple Choices)	[26] 21.3.1			[26] 21.3.1			
9	301 (Moved Permanently)	[26] 21.3.2			[26] 21.3.2			
10	302 (Moved Temporarily)	[26] 21.3.3			[26] 21.3.3			
11	305 (Use Proxy)	[26] 21.3.4			[26] 21.3.4			
12	380 (Alternative Service)	[26] 21.3.5			[26] 21.3.5			
13	400 (Bad Request)	[26] 21.4.1			[26] 21.4.1			
14	401 (Unauthorized)	[26] 21.4.2			[26] 21.4.2			
15	402 (Payment Required)	[26] 21.4.3			[26] 21.4.3			
16	403 (Forbidden)	[26] 21.4.4			[26] 21.4.4			
17	404 (Not Found)	[26] 21.4.5			[26] 21.4.5			
18	405 (Method Not Allowed)	[26] 21.4.6			[26] 21.4.6			
19	406 (Not Acceptable)	[26] 21.4.7			[26] 21.4.7			
20	407 (Proxy Authentication Required)	[26] 21.4.8			[26] 21.4.8			
21	408 (Request Timeout)	[26] 21.4.9			[26] 21.4.9			
22	410 (Gone)	[26] 21.4.10			[26] 21.4.10			
23	413 (Request Entity Too Large)	[26] 21.4.11			[26] 21.4.11			
24	414 (Request-URI Too Large)	[26] 21.4.12			[26] 21.4.12			
25	415 (Unsupported Media Type)	[26] 21.4.13			[26] 21.4.13			
26	416 (Unsupported URI Scheme)	[26] 21.4.14			[26] 21.4.14			
27	420 (Bad Extension)	[26] 21.4.15			[26] 21.4.15			
28	421 (Extension Required)	[26] 21.4.16			[26] 21.4.16			
29	423 (Interval Too Brief)	[26] 21.4.17	с4	c4	[26] 21.4.17	m	m	
30	480 (Temporarily Unavailable)	[26] 21.4.18			[26] 21.4.18			
31	481 (Call/Transaction Does Not Exist)	[26] 21.4.19			[26] 21.4.19			
32	482 (Loop Detected)	[26] 21.4.20			[26] 21.4.20			
33	483 (Too Many Hops)	[26] 21.4.21			[26] 21.4.21			
34	484 (Address Incomplete)	[26] 21.4.22			[26] 21.4.22			
35	485 (Ambiguous)	[26] 21.4.23			[26] 21.4.23			
36	486 (Busy Here)	[26] 21.4.24			[26] 21.4.24			
37	487 (Request Terminated)	[26] 21.4.25			[26] 21.4.25			
38	488 (Not Acceptable Here)	[26] 21.4.26			[26] 21.4.26			
39	489 (Bad Event)	[28] 7.3.2	сЗ	c3	[28] 7.3.2	c3	c3	
40	491 (Request Pending)	[26] 21.4.27			[26] 21.4.27			
41	493 (Undecipherable)	[26] 21.4.28			[26] 21.4.28			
41A	494 (Security Agreement Required)	[48] 2	c5	c5	[48] 2	c6	c6	
42	500 (Internal Server Error)	[26] 21.5.1	1		[26] 21.5.1	1		
43	501 (Not Implemented)	[26] 21.5.2			[26] 21.5.2			
44	502 (Bad Gateway)	[26] 21.5.3			[26] 21.5.3			
45	503 (Service Unavailable)	[26] 21.5.4			[26] 21.5.4			
46	504 (Server Time-out)	[26] 21.5.5			[26] 21.5.5			

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
47	505 (Version not supported)	[26] 21.5.6			[26] 21.5.6				
48	513 (Message Too Large)	[26] 21.5.7			[26] 21.5.7				
49	580 (Precondition Failure)	[30] 8			[30] 8				
50	600 (Busy Everywhere)	[26] 21.6.1			[26] 21.6.1				
51	603 (Decline)	[26] 21.6.2			[26] 21.6.2				
52	604 (Does Not Exist Anywhere)	[26] 21.6.3			[26] 21.6.3				
53	606 (Not Acceptable)	[26] 21.6.4			[26] 21.6.4				
c1:	IF A.5/9 THEN m ELSE n/a	INVITE respo	onse.						
c2:	IF A.5/9 THEN o ELSE n/a INVITE response.								
c3:	IF A.4/20 THEN m ELSE n/s	a SIP specific	event notifica	ation extensi	on.				
c4:	IF A.5/19 OR A.5/21 THEN m ELSE n/a REGISTER response or SUBSCRIBE response.								
oF.							ian nrataaa		

- c5: IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar.
- c6: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.

A.2.1.4.2 ACK method

Prerequisite A.5/1 – ACK request

Table A.7: Supported headers within the ACK request

Item	Header		Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
2	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c2	c2		
3	Authorization	[26] 20.7	с3	c3	[26] 20.7	c3	с3		
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m		
6	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m		
7	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m		
8	Content-Language	[26] 20.13	0	0	[26] 20.13	m	m		
9	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m		
10	Content-Type	[26] 20.15	0	0	[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		
14	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a		
15	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m		
15A	Privacy	[33] 4.2	c6	n/a	[33] 4.2	c6	n/a		
16	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a		
17	Proxy-Require	[26] 20.29	0	n/a	[26] 20.29	n/a	n/a		
18	Require	[26] 20.32	0	0	[26] 20.32	m	m		
19	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a		
20	Timestamp	[26] 20.38	с7	с7	[26] 20.38	m	m		
21	То	[26] 20.39	m	m	[26] 20.39	m	m		
22	User-Agent	[26] 20.41	0	0	[26] 20.41	m	m		
23	Via	[26] 20.42	m	m	[26] 20.42	m	m		
c1: c2:	IF A.4/20 THEN o ELSE n/a SIP specific event notification extension. IF A.4/20 THEN m ELSE n/a SIP specific event notification extension.								

- IF A.4/7 THEN m ELSE n/a - authentication between UA and UA. c3:
- c4: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
- c5:
- IF A.4/8A THEN or ELSE n/a - authentication between UA and proxy.

 IF A.4/26 THEN or ELSE n/a - a privacy mechanism for the Session Initiation Protocol (SIP).

 IF A.4/6 THEN or ELSE n/a - timestamping of requests. c6:
- c7:

Table A.8: Void

A.2.1.4.3 BYE method

Prerequisite A.5/2 - - BYE request

Table A.9: Supported headers within the BYE request

Item	Header	5	Sending		R	eceiving	
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	0	0	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	0	0	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	0	0	[26] 20.3	m	m
3A	Allow	[26] 20.5	0	0	[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	с3	c3	[26] 20.7	сЗ	с3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m
8	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m
9	Content-Language	[26] 20.13	0	0	[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
15	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
16	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m
16A	P-Access-Network-Info	[52] 4.4	c9	c10	[52] 4.4	с9	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
16E	P-Preferred-Identity	[34] 9.2	c6	Х	[34] 9.2	n/a	n/a
16F	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	0	n/a	[26] 20.29	n/a	n/a
19	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
20	Require	[26] 20.32	0	0	[26] 20.32	m	m
21	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
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
22	Supported	[26] 20.37	0	0	[26] 20.37	m	m
23	Timestamp	[26] 20.38	с8	с8	[26] 20.38	m	m
24	То	[26] 20.39	m	m	[26] 20.39	m	m
25	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0
<u> </u>	Via	[26] 20.42	m	m	[20] 20.42	m	m
c1:	IF A.4/20 THEN o ELSE	n/a SIP specific			on.	1	1 ***
c2:	IF A.4/20 THEN m ELSE	n/a SIP specific	event notificat	ion extensi	on.		
c3:	IF A.4/7 THEN m ELSE i	n/a authenticatio	n between UA	and UA.			
c4:	IF A.4/11 THEN o ELSE				onses.		
c5:	IF A.4/8A THEN m ELSE						

- IF A.4/25 THEN o ELSE n/a - private extensions to the Session Initiation Protocol (SIP) for asserted identity c6: within trusted networks.
- IF A.4/26 THEN o ELSE n/a - a privacy mechanism for the Session Initiation Protocol (SIP). c7:
- c8: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
- IF A.4/34 THEN o ELSE n/a - the P-Access-Network-Info header extension. c9: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. c10:
- 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 c11: acting as terminating UA or AS acting as third-party call controller.
- c12: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
- IF A.4/35 THEN o ELSE n/a - the P-Charging-Function-Addresses header extension. c13:
- c14: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
- c15:
- IF A.4/37 THEN o ELSE n/a - security mechanism agreement for the session initiation protocol (note). IF A.4/37 THEN m ELSE n/a - security mechanism agreement for the session initiation protocol. c16:

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].

Table A.10: Void

Prerequisite: A.5/3 - - BYE response

Prerequisite: A.6/1 - - 100 (Trying)

Table A.11: Supported headers within the BYE response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m	
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m	
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m	
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m	
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m	
6	То	[26] 20.39	n/a	n/a	[26] 20.39	m	m	
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m	

Table A.12: Supported headers within the BYE response - all remaining status-codes

2 0 3 0 4 0 5 0	Call-ID Content-Disposition Content-Encoding Content-Language	Ref. [26] 20.8 [26] 20.11 [26] 20.12	RFC status m	Profile status	Ref.	RFC	Profile	
2 0 3 0 4 0 5 0	Content-Disposition Content-Encoding	[26] 20.11	m			status	status	
3 (4 (5 (6 (6 (6 (6 (6 (6 (6 (6 (6 (6 (6 (6 (6	Content-Encoding			m	[26] 20.8	m	m	
3 (4 (5 (6 (6 (6 (6 (6 (6 (6 (6 (6 (6 (6 (6 (6	Content-Encoding	[26] 20 12	0	0	[26] 20.11	m	m	
5 (Content-Language	[20] 20.12	0	0	[26] 20.12	m	m	
6		[26] 20.13	0	0	[26] 20.13	m	m	
	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	
/	Cseq	[26] 20.16	m	m	[26] 20.16	m	m	
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m	
9 1	From	[26] 20.20	m	m	[26] 20.20	m	m	
10 I	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m	
10A I	P-Access-Network-Info	[52] 4.4	c5	с6	[52] 4.4	c5	c6	
10B I	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3	
	P-Charging-Function- Addresses	[52] 4.5	с9	c10	[52] 4.5	с9	c10	
10D I	P-Charging-Vector	[52] 4.6	с8	n/a	[52] 4.6	c8	n/a	
10E I	P-Preferred-Identity	[34] 9.2	c3	Х	[34] 9.2	n/a	n/a	
10F	Privacy	[33] 4.2	c4	n/a	[33] 4.2	c4	c4	
10G I	Require	[26] 20.32	m	m	[26] 20.32	m	m	
10H :	Server	[26] 20.35	0	0	[26] 20.35	0	0	
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2	
12	То	[26] 20.39	m	m	[26] 20.39	m	m	
12A I	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0	
13	Via	[26] 20.42	m	m	[26] 20.42	m	m	
14	Warning	[26] 20.43	o (note)	0	[26] 20.43	0	0	
c1:	IF A.4/11 THEN o ELSE n/a ir	nsertion of da	ate in reques	ts and respo	nses.			
c2:	IF A.4/6 THEN m ELSE n/a tir	mestamping	of requests.					
	IF A.4/25 THEN o ELSE n/a p	rivate extens	sions to the S	Session Initia	tion Protocol	(SIP) for ass	erted	
	identity within trusted networks.				B .	1 (OID)		
	IF A.4/26 THEN 0 ELSE n/a a					coi (SIP).		
	IF A.4/34 THEN 0 ELSE n/a tl					المالية	_	
	IF A.4/34 AND A.3/1 THEN m ELSE n/a the P-Access-Network-Info header extension and UE.							
	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							
c8:	AS acting as terminating UA or AS acting as third-party call controller. IF A.4/36 THEN o ELSE n/a the P-Charging-Vector header extension.							
	IF A.4/35 THEN to ELSE n/a the P-Charging-Function-Addresses header extension.							
	IF A.4/35 THEN m ELSE n/a the P-Charging-Function-Addresses header extension. For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.							

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/6 - - 2xx

Table A.13: Supported headers within the BYE response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
1	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2		
4	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.								

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 (Ambiguous)

Table A.14: Supported headers within the BYE response

Item	Header		Sending		Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
0B	Contact	[26] 20.10	o (note)	0	[26] 20.10	m	m		
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.								

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.15: Supported headers within the BYE response

Item	Header		Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1		
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m		
c1:	c1: IF A.5/7 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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.16: Supported headers within the BYE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
3	Retry-After	[26] 20.33	0	0	[26] 20.33	0	0	
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/18 - - 405 (Method Not Allowed)

Table A.17: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Allow	[26] 20.5	m	m	[26] 20.5	m	m
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite: A.6/19 - - 407 (Proxy Authentication Required)

Table A.18: Supported headers within the BYE response

Item	Header		Sending		Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1		
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
6	WWW-Authenticate	[26] 20.44	0	0	[26] 20.44	0	0		
c1:	IF A.5/7 THEN m ELSE n/a support of authentication between UA and UA.								

Prerequisite A.5/3 - - BYE response

Prerequisite A.6/25 - - 415 (Unsupported Media Type)

Table A.19: Supported headers within the BYE response

Item	Header		Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
1	Accept	[26] 20.1	o.1	0.1	[26] 20.1	m	m		
2	Accept-Encoding	[26] 20.2	0.1	0.1	[26] 20.2	m	m		
3	Accept-Language	[26] 20.3	0.1	0.1	[26] 20.3	m	m		
3A	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
0.1	At least one of these capabilities is supported.								

Prerequisite A.5/3 - - BYE response

Prerequisite: A.6/27 - - 420 (Bad Extension)

Table A.20: Supported headers within the BYE response

Item	Header	Sending				Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
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 - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.20A: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
3	Security-Server	[48] 2	Х	Х	[48] 2	c1	c1
3	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol.						

Prerequisite: A.6/34 - - 484 (Address Incomplete)

Table A.21: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Table A.22: Void

A.2.1.4.4 **CANCEL** method

Prerequisite A.5/4 - - CANCEL request

Table A.23: Supported headers within the CANCEL request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
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	с3	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
12	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
14	Privacy	[33] 4.2	c6	n/a	[33] 4.2	c6	n/a
16	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
18	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
19	Supported	[26] 20.37	0	0	[26] 20.37	m	m
20	Timestamp	[26] 20.38	с8	c8	[26] 20.38	m	m
21	То	[26] 20.39	m	m	[26] 20.39	m	m
22	User-Agent	[26] 20.41	0		[26] 20.41	0	
23	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: c2:	IF A.4/20 THEN o ELSE n/a SIP specific event notification extension. IF A.4/20 THEN m ELSE n/a SIP specific event notification extension.						

- IF A.4/7 THEN m ELSE n/a - authentication between UA and UA. c3:
- c4: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
- IF A.4/26 THEN o ELSE n/a - a privacy mechanism for the Session Initiation Protocol (SIP). c6:
- c8: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.

Table A.24: Void

Prerequisite A.5/5 - - CANCEL response

Table A.25: Supported headers within the CANCEL response - all status-codes

Item	Header		Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	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		
5A	Privacy	[33] 4.2	c3	n/a	[33] 4.2	c3	n/a		
6	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2		
7	То	[26] 20.39	m	m	[26] 20.39	m	m		
7A	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0		
8	Via	[26] 20.42	m	m	[26] 20.42	m	m		
9	Warning	[26] 20.43	o (note)	0	[26] 20.43	0	0		
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).								
NOTE:	For a 606 (Not Acceptable Here	e) response, t	his status is l	RECOMMEN	DED rather t	han OPTION	IAL.		

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/6 - - 200 (OK)

Table A.26: Supported headers within the CANCEL response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
2	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.27: Supported headers within the CANCEL response

Item	Header		Sending		Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

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 - - 404, 413, 480, 500, 503, 600, 603

Table A.28: Supported headers within the CANCEL response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Retry-After	[26] 20.33	0	0	[26] 20.33	0	0	
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/5 - - CANCEL response

Prerequisite: A.6/34 - - 484 (Address Incomplete)

Table A.30: Supported headers within the CANCEL response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Table A.31: Void

A.2.1.4.5 COMET method

Void

A.2.1.4.6 INFO method

Void

A.2.1.4.7 INVITE method

Prerequisite A.5/8 - - INVITE request

Table A.46: Supported headers within the INVITE request

Item	Header		Sending			Receiving	
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	0	0	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	0	0	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	0	0	[26] 20.3	m	m
4	Alert-Info	[26] 20.4	0	0	[26] 20.4	c1	c1
5	Allow	[26] 20.5, [26] 5.1	o (note 1)	0	[26] 20.5, [26] 5.1	m	m
6	Allow-Events	[28] 7.2.2	c2	c2	[28] 7.2.2	c2	c2
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	0	0	[26] 20.9	0	0
11	Contact	[26] 20.10	m	m	[26] 20.10	m	m
12	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m
13	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m
14	Content-Language	[26] 20.13	0	0	[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	0	0	[26] 20.19	0	0
20	From	[26] 20.20	m	m	[26] 20.20	m	m
21	In-Reply-To	[26] 20.21	0	0	[26] 20.21	0	0
22	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
23	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m
24	Organization	[26] 20.25	0	0	[26] 20.25	0	0
24A	P-Access-Network-Info	[52] 4.4	c15	c16	[52] 4.4	c15	c17
24B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	с7	c7
24C	P-Called-Party-ID	[52] 4.2	Х	Х	[52] 4.2	c13	c13
24D	P-Charging-Function- Addresses	[52] 4.5	c20	c21	[52] 4.5	c20	c21
24E	P-Charging-Vector	[52] 4.6	c18	c19	[52] 4.6	c18	c19
25	P-Media-Authorization	[31] 6.1	n/a	n/a	[31] 6.1	c11	c12
25A	P-Preferred-Identity	[34] 9.2	с7	c5	[34] 9.2	n/a	n/a
25B	P-Visited-Network-ID	[52] 4.3	x (note 3)	Х	[52] 4.3	c14	n/a
26	Priority	[26] 20.26	0	0	[26] 20.26	0	0
26A	Privacy	[33] 4.2	с9	с9	[33] 4.2	с9	с9
27	Proxy-Authorization	[26] 20.28	с6	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
29	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	m	m
31	Reply-To	[26] 20.31	0	0	[26] 20.31	0	0
32	Require	[26] 20.32	0	m	[26] 20.32	m	m
33	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
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
34	Subject	[26] 20.36	0	0	[26] 20.36	0	0
35	Supported	[26] 20.37	с8	m	[26] 20.37	m	m

Item	Header		Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
36	Timestamp	[26] 20.38	c10	c10	[26] 20.38	m	m		
37	То	[26] 20.39	m	m	[26] 20.39	m	m		
38	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0		
39	Via	[26] 20.42	m	m	[26] 20.42	m	m		
c1:	IF A.4/12 THEN m ELSE n/a	downloading	of alerting in	formation.					
c2:	IF A.4/20 THEN m ELSE n/a				n.				
c3:	IF A.4/7 THEN m ELSE n/a a								
c4:	IF A.4/11 THEN o ELSE n/a i								
c5:	IF A.3/1 AND A.4/25 THEN o EL	_SE n/a UI	E and private	extensions t	o the Session	n Initiation Pr	otocol		
	(SIP) for asserted identity within trusted networks.								
c6:	IF A.4/8A THEN m ELSE n/a								
c7:	IF A.4/25 THEN o ELSE n/a p	orivate extens	sions to the S	Session Initiat	ion Protocol	(SIP) for ass	erted		
	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.4/6 THEN o ELSE n/a timestamping of requests.								
c11:	IF A.4/19 THEN m ELSE n/a		ns for media	authorization	١.				
c12:	IF A.3/1 THEN m ELSE n/a U								
c13:	IF A.4/32 THEN o ELSE n/a t								
c14:	IF A.4/33 THEN o ELSE n/a t								
c15:	IF A.4/34 THEN o ELSE n/a t								
c16:	IF A.4/34 AND A.3/1 THEN m E								
c17:	IF A.4/34 AND (A.3/7A OR A.3/7				s-Network-In	fo header ext	tension and		
	AS acting as terminating UA or A								
c18:	IF A.4/36 THEN 0 ELSE n/a t								
c19:	IF A.4/36 THEN m ELSE n/a								
c20:	IF A.4/35 THEN 0 ELSE n/a t								
c21:	IF A.4/35 THEN m ELSE n/a						(t A)		
c22:	IF A.4/37 THEN 0 ELSE n/a 5								
c23:	IF A.4/37 THEN m ELSE n/a		nanism agre	ement for the	session initia	ation protoco	I.		
0.1:	At least one of these shall be su		1 (00) :- DEC		\	ODTIONAL			
	The strength of this requirement								
NOTE 2:									
	combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included								
NOTE 3:	from a viewpoint of first usage. The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.								
NOTE 4:	Support of this header in this me						architecture		
INOTE 4.	which is implemented. Use of th								
	defined by 3GPP TS 33.203 [19		ino memou k	ο τιοι αμμιομί	iale lu li le Se	curity mecha	IIIOIII		
<u> </u>	uemieu by Joi F 13 33.203 [19	<u>J·</u>							

Table A.47: Void

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/1 - - 100 (Trying)

Table A.48: Supported headers within the INVITE response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m		
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m		
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m		
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m		
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m		
6	То	[26] 20.39	n/a	n/a	[26] 20.39	m	m		
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m		

NOTE:

Table A.49: Supported headers within the INVITE response - all remaining status-codes

Item	Header		Sending		Receiving				
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m		
1A	Call-Info	[26] 20.9	0	0	[26] 20.9	0	0		
2	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m		
3	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m		
4	Content-Language	[26] 20.13	0	0	[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	0	0	[26] 20.24	m	m		
11	Organization	[26] 20.25	0	0	[26] 20.25	0	0		
11A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7		
11B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3		
11C	P-Charging-Function-	[52] 4.5	c10	c11	[52] 4.5	c11	c11		
	Addresses								
11D	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	с9		
11E	P-Preferred-Identity	[34] 9.2	c3	х	[34] 9.2	n/a	n/a		
11F	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4		
11G	Require	[26] 20.32	m	m	[26] 20.32	m	m		
11H	Server	[26] 20.35	0	0	[26] 20.35	0	0		
12	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2		
13	То	[26] 20.39	m	m	[26] 20.39	m	m		
13A	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0		
14	Via	[26] 20.42	m	m	[26] 20.42	m	m		
15	Warning	[26] 20.43	o (note)	0	[26] 20.43	0	0		
c1:	IF A.4/11 THEN o ELSE n/a -			sts and respo	nses.				
c2:	IF A.4/6 THEN m ELSE n/a								
c3:	IF A.4/25 THEN o ELSE n/a -		sions to the	Session Initia	tion Protocol	(SIP) for ass	serted		
	identity within trusted networks								
c4:	IF A.4/26 THEN o ELSE n/a -					col (SIP).			
c5:	IF A.4/34 THEN o ELSE n/a -						_		
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 -								
c9:	IF A.4/36 THEN m ELSE n/a -								
c10:	IF A.4/35 THEN o ELSE n/a -								
c11:	IF A.4/35 THEN m ELSE n/a -	 the P-Chargi 	ina-Function	 Addresses h 	eader extens	ion.			

IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.

For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.

Prerequisite: A.6/2 OR A.6/3 OR A.6/4 OR A.6/5 - - 1xx

Table A.50: Supported headers within the INVITE response

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m
4	Contact	[26] 20.10	0	m	[26] 20.10	m	m
6	P-Media-Authorization	[31] 6.1	n/a	n/a	[31] 6.1	c11	c12
9	Rseq	[27] 7.1	c2	m	[27] 7.1	c3	m
11	Supported	[26] 20.37	0	0	[26] 20.37	m	m
c2:	IF A.4/14 THEN o ELSE n/a ı	reliability of p	rovisional res	sponses in SI	P.		
c3:	IF A.4/14 THEN m ELSE n/a reliability of provisional responses in SIP.						
c11:	IF A.4/19 THEN m ELSE n/a SIP extensions for media authorization.						
c12:	IF A.3/1 THEN m ELSE n/a L	JE.					

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/6 - - 2xx

Table A.51: Supported headers within the INVITE response

ltem	Header		Sending			Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Accept	[26] 20.1	0	0	[26] 20.1	m	m	
1A	Accept-Encoding	[26] 20.2	0	0	[26] 20.2	m	m	
1B	Accept-Language	[26] 20.3	0	0	[26] 20.3	m	m	
2	Allow	[26] 20.5	o (note 1)	0	[26] 20.5	m	m	
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	
8	P-Media-Authorization	[31] 6.1	n/a	n/a	[31] 6.1	c11	c12	
9	Record-Route	[26] 20.30	m	m	[26] 20.30	m	m	
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.							
c11:	IF A.4/19 THEN m ELSE n/a SIP extensions for media authorization.							
c12·	IF A 3/1 THEN m FLSE n/a -	- UF						

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 (Ambiguous)

NOTE 1: The strength of this requirement in RFC 3261 [26] is RECOMMENDED, rather than OPTIONAL

Table A.52: Supported headers within the INVITE response

Item	Header	Sending			Receiving					
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status			
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m			
4	Contact	[26] 20.10	o (note 1)	0	[26] 20.10	m	m			
5	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0			
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m			
NOTE:	The strength of this requirement	The strength of this requirement is RECOMMENDED rather than OPTIONAL.								

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.53: Supported headers within the INVITE response

Item	Header	Sending R					Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
6	Proxy-Authenticate	[26] 20.27	c3	c3	[26] 20.27	c3	c3	
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
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.5/7 THEN m ELSE n/a s	support of aut	hentication b	etween UA a	ind UA.			

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 - - 404, 413, 480, 486, 600, 603

Table A.54: Supported headers within the INVITE response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
8	Retry-After	[26] 20.33	0	0	[26] 20.33	0	0	
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/18 - - 405 (Method Not Allowed)

Table A.55: Supported headers within the INVITE response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
2	Allow	[26] 20.5	m	m	[26] 20.5	m	m		
5	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m		

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/20 - - 407 (Proxy Authentication Required)

Table A.56: Supported headers within the INVITE response

Item	Header		Sending		Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
6	Proxy-Authenticate	[26] 20.27	0		[26] 20.27	0			
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
11	WWW-Authenticate	[26] 20.44	0	0	[26] 20.44	0	0		
c1:	IF A.5/7 THEN m ELSE n/a support of authentication between UA and UA.								

Prerequisite: A.6/25 - - 415 (Unsupported Media Type)

Table A.57: Supported headers within the INVITE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Accept	[26] 20.1	0.1	0.1	[26] 20.1	m	m	
2	Accept-Encoding	[26] 20.2	0.1	0.1	[26] 20.2	m	m	
3	Accept-Language	[26] 20.3	0.1	0.1	[26] 20.3	m	m	
3A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
6	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
11	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
0.1	At least one of these capabili	ties is supported	d.					

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/27 - - 420 (Bad Extension)

Table A.58: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m
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 - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.58A: Supported headers within the INVITE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
3	Security-Server	[48] 2	Х	Х	[48] 2	c1	c1	
3	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
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.6/34 - - 484 (Address Incomplete)

Table A.59: Supported headers within the INVITE response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite: A.6/42 - - 500 (Server Internal Error)

Table A.60: Supported headers within the INVITE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
8	Retry-After	[26] 20.33	m	m	[26] 20.33	0	0	
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/45 - - 503 (Service Unavailable)

Table A.61: Supported headers within the INVITE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
8	Retry-After	[26] 20.33	0	0	[26] 20.33	0	m	
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Table A.62: Void

A.2.1.4.7A MESSAGE method

Prerequisite A.5/9A - - MESSAGE request

Table A.62A: Supported headers within the MESSAGE request

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Allow	[26] 20.5	0	0	[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	0	0	[26] 20.9	0	0
6	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m
7	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m
8	Content-Language	[26] 20.13	0	0	[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	0	0	[26] 20.19	0	0
14	From	[26] 20.20	m	m	[26] 20.20	m	m
15	In-Reply-To	[26] 20.21	0	0	[26] 20.21	0	0
16	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
17	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m
18	Organization	[26] 20.25	0	0	[26] 20.25	0	0
18A	P-Access-Network-Info	[52] 4.4	c15	c16	[52] 4.4	c15	c16
18B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c11	c11
18C	P-Called-Party-ID	[52] 4.2	Х	Х	[52] 4.2	c13	c13
18D	P-Charging-Function- Addresses	[52] 4.5	c20	c21	[52] 4.5	c20	c21
18E	P-Charging-Vector	[52] 4.6	c18	c19	[52] 4.6	c18	c19
18F	P-Preferred-Identity	[34] 9.2	c11	c7	[34] 9.2	n/a	n/a
18G	P-Visited-Network-ID	[52] 4.3	x (note 1)	X	[52] 4.3	c14	n/a
19	Priority	[26] 20.26	0	0	[26] 20.26	0	0
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	0	n/a	[26] 20.29	n/a	n/a
22	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
23	Reply-To	[26] 20.31	0	0	[26] 20.31	0	0
24	Require	[26] 20.32	с8	0	[26] 20.32	m	m
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
26	Subject	[26] 20.35	0	0	[26] 20.36	0	0
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	То	[26] 20.39	m	m	[26] 20.39	m	m
30	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0
31	Via	[26] 20.42	m	m	[26] 20.42	m	m

Item	Header		Sending		Receiving				
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
c1:	IF A.4/20 THEN o ELSE n/a S	SIP specific e	event notificat	ion extension	٦.				
c2:	IF A.4/20 THEN m ELSE n/a	SIP specific	event notifica	tion extensio	n.				
c3:	IF A.4/7 THEN m ELSE n/a a								
c4:	IF A.4/11 THEN o ELSE n/a i	nsertion of da	ate in reques	ts and respor	nses.				
c5:	IF A.162/8A THEN m ELSE i authentication between UA and proxy.								
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.4/14 THEN o.1 ELSE o F	Reliable trans	sport.						
c9:	IF IF A.4/14 THEN o.1 ELSE o -	- support of	reliable trans	port.					
c10:	IF A.4/6 THEN o ELSE n/a tin								
c11:	IF A.4/25 THEN o ELSE n/a p	rivate extens	sions to the S	Session Initiat	tion Protocol	(SIP) for ass	erted		
	identity within trusted networks.								
c12:	IF A.4/26 THEN o ELSE n/a a				nitiation Proto	ocol (SIP).			
c13:	IF A.4/32 THEN o ELSE n/a t		,						
c14:	IF A.4/33 THEN o ELSE n/a t								
c15:	IF A.4/34 THEN o ELSE n/a t								
c16:	IF A.4/34 AND A.3/1 THEN m E								
c17:	IF A.4/34 AND (A.3/7A OR A.3/7				s-Network-In	fo header ext	tension and		
	AS acting as terminating UA or A								
c18:	IF A.4/36 THEN o ELSE n/a t								
c19:	IF A.4/36 THEN m ELSE n/a								
c20:	IF A.4/35 THEN o ELSE n/a t								
c21:	IF A.4/35 THEN m ELSE n/a						()		
c22:	IF A.4/37 THEN o ELSE n/a s								
c23:	IF A.4/37 THEN m ELSE n/a						l.		
	The strength of this requirement								
NOTE 2:	Support of this header in this me								
	which is implemented. Use of this		this method is	s not appropr	iate to the se	ecurity mecha	ınısm		
	defined by 3GPP TS 33.203 [19]								

Table A.62B: Void

Prerequisite A.5/9B - - MESSAGE response

Table A.62C: Supported headers within the MESSAGE response - all remaining status-codes

1 2 3		Ref.	RFC	D (11			
2			KFC	Profile	Ref.	RFC	Profile
2			status	status		status	status
	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
3	Call-Info	[26] 20.9	0	0	[26] 20.9	0	0
	Content-Disposition	[26] 20.11	o (note 2)	o (note 2)	[26] 20.11	m (note 2)	m (note 2)
4	Content-Encoding	[26] 20.12	o (note 2)	o (note 2)	[26] 20.12	m (note 2)	m (note 2)
5	Content-Language	[26] 20.13	o (note 2)	o (note 2)	[26] 20.13	m (note 2)	m (note 2)
6	Content-Length	[26] 20.14	m (note 2)	m (note 2)	[26] 20.14	m (note 2)	m (note 2)
7	Content-Type	[26] 20.15	m (note 2)	m (note 2)	[26] 20.15	m (note 2)	m (note 2)
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	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m
12	Organization	[26] 20.25	0	0	[26] 20.25	0	0
12A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7
12B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
12C	P-Charging-Function- Addresses	[52] 4.5	c10	c11	[52] 4.5	c10	c11
12D	P-Charging-Vector	[52] 4.6	c8	с9	[52] 4.6	с8	с9
12E	P-Preferred-Identity	[34] 9.2	c3	Х	[34] 9.2	n/a	n/a
12F	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4
12G	Require	[26] 20.32	0	0	[26] 20.32	m	m
13	Server	[26] 20.35	0	0	[26] 20.35	0	0
14	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
15	То	[26] 20.39	m	m	[26] 20.39	m	m
16	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0
17	Via	[26] 20.42	m	m	[26] 20.42	m	m
18	Warning	[26] 20.43	0	0	[26] 20.43	0	0

- 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.
- NOTE 1: For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.

NOTE 2: 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.6/6 - - 2xx

Table A.62D: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2	
4	Supported	[26] 20.37	0	0	[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 a	uthentication	between UA	and UA.				

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 (Ambiguous)

Table A.62E: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
2	Contact	[26] 20.10	o (note)	0	[26] 20.10	m	m		
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.								

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.62F: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving					
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status			
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m			
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0			
3	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1			
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m			
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m			
c1:	IF A.5/7 THEN m ELSE n/a support of authentication between UA and UA.									

Prerequisite A.5/9B - - MESSAGE response

 $Prerequisite: A.6/17 \ OR \ A.6/23 \ OR \ A.6/30 \ OR \ A.6/36 \ OR \ A.6/42 \ OR \ A.6/45 \ OR \ A.6/50 \ OR \ A.6/51 \ -- \ 404, \ 413, \ 480, \ A.6/30 \ OR \ A.6/30$

486, 500, 503, 600, 603

Table A.62G: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving			
		Ref.	Ref. RFC Profile			RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Retry-After	[26] 20.33	0	0	[26] 20.33	0	0	
5	Supported	[26] 20 37	m	m	[26] 20 37	m	m	

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/18 - - 405 (Method Not Allowed)

Table A.62H: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving		
		Ref. RFC Profile			Ref.	RFC	Profile
			status	status		status	status
1	Allow	[26] 20.5	m	m	[26] 20.5	m	m
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/20 - - 407 (Proxy Authentication Required)

Table A.62I: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving					
		Ref.	RFC	Profile	Ref.	RFC	Profile			
			status	status		status	status			
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m			
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0			
3	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1			
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m			
6	WWW-Authenticate	[26] 20.44	0	0	[26] 20.44	0	0			
c1:	c1: IF A.5/7 THEN m ELSE n/a support of authentication between UA and UA.									

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/25 - - 415 (Unsupported Media Type)

Table A.62J: Supported headers within the MESSAGE response

Item	Header	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	0.1	[26] 20.2	m	m		
3	Accept-Language	[26] 20.3	o.1	0.1	[26] 20.3	m	m		
4	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
5	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
0.1	At least one of these capabilities is supported.								

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/27 - - 420 (Bad Extension)

Table A.62K: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
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 - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.62L: Supported headers within the MESSAGE response

Item	Header	Sending				Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
3	Security-Server	[48] 2	Х	х	[48] 2	c1	c1	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
c1:	IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol.							

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/34 - - 484 (Address Incomplete)

Table A.62M: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving			
		Ref. RFC Profile			Ref.	RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Table A.62N: Void

A.2.1.4.8 NOTIFY method

Prerequisite A.5/10 - - NOTIFY request

Table A.63: Supported headers within the NOTIFY request

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Accept	[26] 20.1	0	0	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	0	0	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	0	0	[26] 20.3	m	m
3A	Allow	[26] 20.5	0	0	[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	с3	[26] 20.7	c3	с3
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6A	Contact	[26] 20.10	m	m	[26] 20.10	m	m
7	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m
8	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m
9	Content-Language	[26] 20.13	0	0	[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	From	[26] 20.20	m	m	[26] 20.20	m	m
16	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
17	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m
17A	P-Access-Network-Info	[52] 4.4	c10	c11	[52] 4.4	c10	c12
17B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[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
17E	P-Preferred-Identity	[34] 9.2	c6	X	[34] 9.2	n/a	n/a
17F	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	0	n/a	[26] 20.29	n/a	n/a
20	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	c9	c9
21	Require	[26] 20.32	0	0	[26] 20.32	m	m
22A	Security-Client	[48] 2.3.1	c16	c16	[48] 2.3.1	n/a	n/a
22B	Security-Verify	[48] 2.3.1	c17	c17	[48] 2.3.1	n/a	n/a
22	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
23	Subscription-State	[28] 8.2.3	m	m	[28] 8.2.3	m	m
24	Supported	[26] 20.37	0	0	[26] 20.37	m	m
25	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m
26	То	[26] 20.39	m	m	[26] 20.39	m	m
27	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0
28	Via	[26] 20.42	m	m	[26] 20.42	m	m

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 THEN o ELSE n/a security mechanism agreement for the session initiation protocol (note).
c17:	IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol.
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			
c1:										

Table A.65: Supported headers within the NOTIFY response - all status-codes

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m
4	Content-Language	[26] 20.13	0	0	[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	0	0	[26] 20.24	m	m
10A	P-Access-Network-Info	[52] 4.4	c5	с6	[52] 4.4	c5	с7
10B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3
10C	P-Charging-Function-	[52] 4.5	с9	c10	[52] 4.5	с9	c10
	Addresses				' '		
10D	P-Charging-Vector	[52] 4.6	с8	n/a	[52] 4.6	с8	n/a
10E	P-Preferred-Identity	[34] 9.2	c3	х	[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	0	0	[26] 20.35	0	0
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
12	То	[26] 20.39	m	m	[26] 20.39	m	m
12A	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0
13	Via	[26] 20.42	m	m	[26] 20.42	m	m
14	Warning	[26] 20.43	o (note)	0	[26] 20.43	0	0
c1:	IF A.4/11 THEN o ELSE n/a i			ts and respon		•	1
c2:	IF A.4/6 THEN m ELSE n/a ti			•			
c3:	IF A.4/25 THEN o ELSE n/a p	orivate exten	sions to the S	Session Initia	tion Protocol	(SIP) for ass	erted
	identity within trusted networks.						
c4:	IF A.4/26 THEN o ELSE n/a a	a privacy med	chanism for t	he Session Ir	nitiation Proto	col (SIP).	
c5:	IF A.4/34 THEN o ELSE n/a t	he P-Access	-Network-Inf	o header exte	ension.		
c6:	IF A.4/34 AND A.3/1 THEN m E						
c7:	IF A.4/34 AND (A.3/7A OR A.3/7				s-Network-In	fo header ex	tension and
	AS acting as terminating UA or A						
c8:	IF A.4/36 THEN o ELSE n/a t						
c9:	IF A.4/35 THEN o ELSE n/a t						
c10:	IF A.4/35 THEN m ELSE n/a						
NOTE:	For a 606 (Not Acceptable Here) response, t	his status is l	RECOMMEN	DED rather t	han OPTION	IAL.

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/6 and A.6/7 - - 2xx

Table A.66: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	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	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.

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 (Ambiguous)

Table A.67: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Contact	[26] 20.10	m (note)	m	[26] 20.10	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
NOTE:	The strength of this requirement	t is RECOMM	IENDED rath	er than MAN	DATORY for	a 485 respo	nse.	

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.68: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving					
		Ref.	RFC	Profile	Ref.	RFC	Profile			
			status	status		status	status			
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m			
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0			
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1			
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m			
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m			
c1:	IF A.5/7 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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.69: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
			Status	รเลเนร		Status	รเสเนร	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
3	Retry-After	[26] 20.33	0	0	[26] 20.33	0	0	
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/18 -- 405 (Method Not Allowed)

Table A.70: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	m	m	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite: A.6/20 - - 407 (Proxy Authentication Required)

Table A.71: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
2	Proxy-Authenticate	[26] 20.27	c3	c3	[26] 20.27	с3	c3	
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
6	WWW-Authenticate	[26] 20.44	0	0	[26] 20.44	0	0	
c3:	IF A.5/7 THEN m ELSE n/a s	support of aut	hentication b	etween UA a	nd UA.			

Prerequisite A.5/11 - - NOTIFY response

Prerequisite A.6/25 - - 415 (Unsupported Media Type)

Table A.72: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Accept	[26] 20.1	0.1	o.1	[26] 20.1	m	m	
2	Accept-Encoding	[26] 20.2	0.1	o.1	[26] 20.2	m	m	
3	Accept-Language	[26] 20.3	0.1	o.1	[26] 20.3	m	m	
3A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/27 - - 420 (Bad Extension)

Table A.73: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
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 - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.73A: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
3	Security-Server	[48] 2	Х	х	[48] 2	c1	c1		
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
c1:	IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol.								

Prerequisite: A.6/34 - - 484 (Address Incomplete)

Table A.74: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/11 - - NOTIFY response

Prerequisite: A.6/39 - - 489 (Bad Event)

Table A.75: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	m	m	
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	

Table A.76: Void

A.2.1.4.9 OPTIONS method

Prerequisite A.5/12 - - OPTIONS request

Table A.77: Supported headers within the OPTIONS request

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Accept	[26] 20.1	m	m	[26] 20.1	m	m
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	0	0	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c1	c1	[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	0	0	[26] 20.9	0	0
8	Contact	[26] 20.10	0	0	[26] 20.10	0	0
9	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m
10	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m
11	Content-Language	[26] 20.13	0	0	[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	From	[26] 20.20	m	m	[26] 20.20	m	m
17	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
18	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m
19	Organization	[26] 20.25	0	0	[26] 20.25	0	0
19A	P-Access-Network-Info	[52] 4.4	c11	c12	[52] 4.4	c11	c13
19B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c6	c6
19C	P-Called-Party-ID	[52] 4.2	Х	х	[52] 4.2	с9	c9
19D	P-Charging-Function- Addresses	[52] 4.5	c16	c17	[52] 4.5	c16	c17
19E	P-Charging-Vector	[52] 4.6	c14	c15	[52] 4.6	c14	c15
19F	P-Preferred-Identity	[34] 9.2	c6	c4	[34] 9.2	n/a	n/a
19G	P-Visited-Network-ID	[52] 4.3	x (note 2)	х	[52] 4.3	c10	n/a
19H	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	0	o (note 1)	[26] 20.29	n/a	n/a
22	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a
23	Require	[26] 20.32	0	0	[26] 20.32	m	m
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
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	То	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0
29	Via	[26] 20.42	m	m	[26] 20.42	m	m

 c2: IF A.4/20 THEN m ELSE n/a SIP specific event notification extension. 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 the P-Called-Party-ID extension. 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-Access-Network-ID extension. c11: IF A.4/34 THEN o ELSE n/a the P-Access-Network-Info header extension and UE. c13: 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.3/1 THEN m ELSE n/a the P-Charging-Vector header extension. c14: IF A.4/36 THEN o ELSE n/a the P-Charging-Vector header extension. c15: IF A.4/35 THEN m ELSE n/a the P-Charging-Function-Addresses header extension. c16: IF A.4/35 THEN m ELSE n/a the P-Charging-Function-Addresses header extension. c17: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol (note 3). IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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		
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.4/25 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 number of the protocol (SIP). c13: 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) 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. 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-Function-Addresses 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 security mechanism agreement for the session initiation protocol (note 3). IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [52] is SHOULD NOT, rather than MUST NOT.	c1:	IF A.4/20 THEN m ELSE n/a SIP specific event notification extension.
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.4/3C THEN o ELSE n/a the P-Called-Party-ID extension. 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-Access-Network-Info header 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) 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. c14: IF A.4/36 THEN o ELSE n/a the P-Charging-Vector header extension. c15: IF A.4/35 THEN o ELSE n/a the P-Charging-Function-Addresses 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 or ELSE n/a security mechanism agreement for the session initiation protocol (note 3). IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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	c2:	IF A.4/7 THEN m ELSE n/a authentication between UA and UA.
(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 and UE. c13: IF A.4/34 AND A.3/1 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. 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 m 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 THEN m ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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	c3:	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 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 and UE. 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) 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. 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-Function-Addresses header extension. c16: IF A.4/35 THEN m ELSE n/a the P-Charging-Function-Addresses header extension. c17: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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	c4:	IF A.3/1 AND A.4/25 THEN o ELSE n/a UE and private extensions to the Session Initiation Protocol
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 and UE. c13: IF A.4/34 AND A.3/1 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. 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 o ELSE n/a the P-Charging-Function-Addresses header extension. c18: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol (note 3). IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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		(SIP) for asserted identity within trusted networks.
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.4/26 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 and UE. 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) 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. 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-Function-Addresses header extension. c16: IF A.4/35 THEN m ELSE n/a the P-Charging-Function-Addresses header extension. c17: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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	c5:	IF A.4/8A THEN m ELSE n/a authentication between UA and proxy.
 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) 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. 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 THEN m ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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 	c6:	IF A.4/25 THEN o ELSE n/a private extensions to the Session Initiation Protocol (SIP) for asserted
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) 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. c14: IF A.4/36 THEN o ELSE n/a the P-Charging-Vector header extension. c15: IF A.4/35 THEN m ELSE n/a the P-Charging-Function-Addresses 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 THEN o ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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		identity within trusted networks.
 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) 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. 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 THEN m ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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 	c7:	IF A.4/6 THEN o ELSE n/a timestamping of requests.
 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) 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. 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-Function-Addresses 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 o ELSE n/a the P-Charging-Function-Addresses header extension. c18: IF A.4/37 THEN o ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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 	c8:	IF A.4/26 THEN o ELSE n/a a privacy mechanism for the Session Initiation Protocol (SIP).
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) 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. 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 THEN o ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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	c9:	IF A.4/32 THEN o ELSE n/a the P-Called-Party-ID 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) 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. 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 THEN o ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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 	c10:	IF A.4/33 THEN o ELSE n/a the P-Visited-Network-ID extension.
c13: 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. 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 THEN o ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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	c11:	IF A.4/34 THEN o ELSE n/a the P-Access-Network-Info header extension.
AS acting as terminating UA or AS acting as third-party call controller. 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 THEN o ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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	c12:	
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 THEN o ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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	c13:	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
 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 THEN o ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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 		
 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 THEN o ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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 	c14:	
 c17: IF A.4/35 THEN m ELSE n/a the P-Charging-Function-Addresses header extension. c18: IF A.4/37 THEN o ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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 	c15:	
c18: IF A.4/37 THEN o ELSE n/a security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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	c16:	
 c19: IF A.4/37 THEN m ELSE n/a security mechanism agreement for the session initiation protocol. 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 3455 [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 	c17:	
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 3455 [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		
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 3455 [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		
from a viewpoint of first usage. NOTE 2: The strength of this requirement in RFC 3455 [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	NOTE 1:	
NOTE 2: The strength of this requirement in RFC 3455 [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		
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		
which is implemented. Use of this header in this method is not appropriate to the security mechanism		
	NOTE 3:	
defined by 3GPP TS 33.203 [19].		which is implemented. Use of this header in this method is not appropriate to the security mechanism
		defined by 3GPP TS 33.203 [19].

Table A.78: Void

Prerequisite: A.6/1 - - 100 (Trying)

Table A.79: Supported headers within the OPTIONS response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m	
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m	
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m	
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m	
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m	
6	То	[26] 20.39	n/a	n/a	[26] 20.39	m	m	
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m	

Receiving

Prerequisite A.5/13 - - OPTIONS response

Item

Header

Table A.80: Supported headers within the OPTIONS response - all remaining status-codes

		Ref.	RFC	Profile	Ref.	RFC	Profile			
			status	status		status	status			
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m			
1A	Call-Info	[26] 20.9	0	0	[26] 20.9	0	0			
2	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m			
3	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m			
4	Content-Language	[26] 20.13	0	0	[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	Sseq [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	0	0	[26] 20.24	m	m			
11	Organization	[26] 20.25	0	0	[26] 20.25	0	0			
11A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7			
11B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3			
11C	P-Charging-Function- Addresses	[52] 4.5	c10	c11	[52] 4.5	c10	c11			
11D	P-Charging-Vector	[52] 4.6	c8	с9	[52] 4.6	с8	с9			
11E	P-Preferred-Identity	[34] 9.2	c3	X	[34] 9.2	n/a	n/a			
11F	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4			
11G	Require	[26] 20.32	m	m	[26] 20.32	m	m			
12	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2			
13	То	[26] 20.39	m	m	[26] 20.39	m	m			
13A	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0			
14	Via	[26] 20.42	m	m	[26] 20.42	m	m			
15	Warning	[26] 20.43	o (note)	0	[26] 20.43	0	0			
c1:	IF A.4/11 THEN o ELSE n/a i	nsertion of da	ate in reques	ts and respor	nses.					
c2:	IF A.4/6 THEN m ELSE n/a ti	mestamping	of requests.	•						
c3:	IF A.4/25 THEN o ELSE n/a p	orivate extens	sions to the S	Session Initiat	tion Protocol	(SIP) for ass	erted			
	identity within trusted networks.									
c4:	IF A.4/26 THEN o ELSE n/a a					col (SIP).				
c5:	IF A.4/34 THEN o ELSE n/a t									
c6:	IF A.4/34 AND A.3/1 THEN m E									
c7:	IF A.4/34 AND (A.3/7A OR A.3/7				s-Network-In	fo header ext	tension and			
-0-	AS acting as terminating UA or A				_					
c8:	IF A.4/36 THEN 0 ELSE n/a t									
c9:	IF A.4/36 THEN m ELSE n/a					00				
c10:	IF A.4/35 THEN to ELSE n/a t									
c11:	IF A.4/35 THEN m ELSE n/a						Δ1			
NOTE:	For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.									

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/6 - - 2xx

Table A.81: Supported headers within the OPTIONS response

Item	Header		Sending		Receiving				
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
1	Accept	[26] 20.1	m	m	[26] 20.1	m	m		
2	Allow	[26] 20.5	o (note 1)	0	[26] 20.5	m	m		
3	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2		
5	Contact	[26] 20.10	0		[26] 20.10	0			
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
c1:	IF A.4/7 THEN o ELSE n/a au	uthentication	between UA	and UA.					
c2:	IF A.4/7 THEN m ELSE n/a authentication between UA and UA.								
NOTE 1:	The strength of this requirement in RFC 3261 [26] is RECOMMENDED, rather than OPTIONAL.								

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 (Ambiguous)

Table A.82: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving					
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status			
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m			
3	Contact	[26] 20.10	o (note)	0	[26] 20.10	m	m			
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0			
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m			
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.									

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.83: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving						
		Ref.	RFC	Profile	Ref.	RFC	Profile				
			status	status		status	status				
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m				
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0				
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1				
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m				
10	WWW-Authenticate	[26] 20.44	0		[26] 20.44	0					
c1:											

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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.84: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
5	Retry-After	[26] 20.33	0	0	[26] 20.33	0	0	
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/18 - - 405 (Method Not Allowed)

Table A.85: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
			อเลเนอ	อเลเนอ		อเลเนอ	อเลเนอ	
2	Allow	[26] 20.5	m	m	[26] 20.5	m	m	
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite: A.6/20 - - 407 (Proxy Authentication Required)

Table A.86: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving					
		Ref.	RFC	Profile	Ref.	RFC	Profile			
			status	status		status	status			
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m			
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0			
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1			
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m			
8	WWW-Authenticate	[26] 20.44	0	0	[26] 20.44	0	0			
c1:	IF A.5/7 THEN m ELSE n/a support of authentication between UA and UA.									

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/25 - - 415 (Unsupported Media Type)

Table A.87: Supported headers within the OPTIONS response

Item	Header		Sending			Receiving										
		Ref.	RFC	Profile	Ref.	RFC	Profile									
			status	status		status	status									
1	Accept	[26] 20.1	0.1	0.1	[26] 20.1	m	m									
2	Accept-Encoding	[26] 20.2	0.1	0.1	[26] 20.2	m	m									
3	Accept-Language	[26] 20.3	o.1	0.1	[26] 20.3	m	m									
4	Allow	[26] 20.5	0	0	[26] 20.5	m	m									
5	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0									
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m									
0.1	At least one of these capabilities	s is supported	d.				At least one of these capabilities is supported.									

Prerequisite A.5/13 - - OPTIONS response

Prerequisite: A.6/27 - - 420 (Bad Extension)

Table A.88: Supported headers within the OPTIONS response

Item	Header		Sending		Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
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 - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.88A: Supported headers within the OPTIONS response

Item	Header			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
3	Security-Server	[48] 2	Х	Х	[48] 2	c1	c1
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF A.4/37 THEN m ELSE n/a -	- security med	hanism agre	ement for the	e session initia	ation protoco	l.

Prerequisite: A.6/34 - - 484 (Address Incomplete)

Table A.89: Supported headers within the OPTIONS response

Item	Header		Sending		Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Table A.90: Void

A.2.1.3.10 PRACK method

Prerequisite A.5/14 - - PRACK request

c14:

Table A.91: Supported headers within the PRACK request

ltem	Header		Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
1	Accept	[26] 20.1	0	0	[26] 20.1	m	m		
2	Accept-Encoding	[26] 20.2	0	0	[26] 20.2	m	m		
3	Accept-Language	[26] 20.3	0	0	[26] 20.3	m	m		
3A	Allow	[26] 20.5	0	0	[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	с3		
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m		
7	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m		
8	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m		
9	Content-Language	[26] 20.13	0	0	[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		
15	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a		
16	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m		
16A	P-Access-Network-Info	[52] 4.4	c9	c10	[52] 4.4	c9	c11		
16B	P-Charging-Function-	[52] 4.5	c13	c14	[52] 4.5	c13	c14		
	Addresses	[02]			[02]				
16C	P-Charging-Vector	[52] 4.6	c12	n/a	[52] 4.6	c12	n/a		
16D	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	0	n/a	[26] 20.29	n/a	n/a		
19	RAck	[27] 7.2	m	m	[27] 7.2	m	m		
20	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a		
21	Require	[26] 20.32	0	0	[26] 20.32	m	m		
22	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a		
23	Supported	[26] 20.37	0	0	[26] 20.37	m	m		
24	Timestamp	[26] 20.38	c8	c8	[26] 20.38	m	m		
25	То	[26] 20.39	m	m	[26] 20.39	m	m		
26	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0		
27	Via	[26] 20.42	m	m	[26] 20.42	m	m		
c1:	IF A.4/20 THEN o ELSE n/a					1	1		
c2:	IF A.4/20 THEN m ELSE n/a								
c3:	IF A.4/7 THEN m ELSE n/a a								
c4:	IF A.4/11 THEN o ELSE n/a				nses.				
c5:	IF A.4/8A THEN m ELSE n/a								
c6:	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 THEN m E	LSE n/a th	ne P-Access-	Network-Info	header exte	nsion and UI	E.		
c11:	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								
c12:	IF A.4/36 THEN o ELSE n/a								
c13:	IF A.4/35 THEN o ELSE n/a								
c1.4·	IE A 4/25 THEN IN ELSE N/O	the D Chargi	na Eupotion	Addrosos b		ion			

IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.

Table A.92: Void

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/1 - - 100 (Trying)

Table A.93: Supported headers within the PRACK response

Item	Header	Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m	
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m	
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m	
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m	
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m	
6	То	[26] 20.39	n/a	n/a	[26] 20.39	m	m	
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m	

Table A.94: Supported headers within the PRACK response - all remaining status-codes

Item	Header		Sending			Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m	
2	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m	
3	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m	
4	Content-Language	[26] 20.13	0	0	[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	0	0	[26] 20.24	m	m	
10A	P-Access-Network-Info	[52] 4.4	c3	c4	[52] 4.4	c3	c5	
10B	P-Charging-Function-	[52] 4.5	с7	с8	[52] 4.5	с7	c8	
	Addresses							
10C	P-Charging-Vector	[52] 4.6	c6	n/a	[52] 4.6	c6	n/a	
10D	Privacy	[33] 4.2	c2	n/a	[33] 4.2	c2	n/a	
10E	Require	[26] 20.32	0	0	[26] 20.32	m	m	
10F	Server	[26] 20.35	0	0	[26] 20.35	0	0	
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2	
12	То	[26] 20.39	m	m	[26] 20.39	m	m	
12A	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0	
13	Via	[26] 20.42	m	m	[26] 20.42	m	m	
14	Warning	[26] 20.43	o (note)	0	[26] 20.43	0	0	
c1:	IF A.4/11 THEN o ELSE n/a i	nsertion of da	ate in reques	ts and respor	nses.			
c2:	IF A.4/26 THEN o ELSE n/a a	a privacy med	chanism for t	he Session Ir	nitiation Proto	col (SIP).		
c3:	IF A.4/34 THEN o ELSE n/a t	he P-Access	-Network-Inf	o header exte	ension.			
c4:	IF A.4/34 AND A.3/1 THEN m E							
c5:	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.							
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							
NOTE:	For a 606 (Not Acceptable Here) response, t	his status is l	RECOMMEN	DED rather t	han OPTION	IAL.	

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/6 - - 2xx

Table A.95: Supported headers within the PRACK response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
0B	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2	
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 a	uthentication	between UA	and UA.				

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 (Ambiguous)

Table A.96: Supported headers within the PRACK response

Item	Header		Sending		Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
1	Contact	[26] 20.10	o (note)	0	[26] 20.10	m	m		
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.								

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.97: Supported headers within the PRACK response

Item	Header	Sending				Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1		
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m		
c1:	IF A.5/7 THEN m ELSE n/a s	support of aut	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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.98: Supported headers within the PRACK response

Item	Header		Sending		Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
3	Retry-After	[26] 20.33	0	0	[26] 20.33	0	0
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/18 - - 405 (Method Not Allowed)

Table A.99: Supported headers within the PRACK response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	m	m	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite: A.6/20 - - 407 (Proxy Authentication Required)

Table A.100: Supported headers within the PRACK response

Item	Header	Sending			Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1		
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
6	WWW-Authenticate	[26] 20.44	0	0	[26] 20.44	0	0		
c1:	IF A.5/7 THEN m ELSE n/a support of authentication between UA and UA.								

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/25 - - 415 (Unsupported Media Type)

Table A.101: Supported headers within the PRACK response

Item	Header	Sending			Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Accept	[26] 20.1	0.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	0.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	0.1	o.1	[26] 20.3	m	m
3A	Allow	[26] 20.5	0	0	[26] 20.5	m	m
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/27 - - 420 (Bad Extension)

Table A.102: Supported headers within the PRACK response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/15 - - PRACK response

Prerequisite: A.6/28 OR A.6/41A - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.102A: Supported headers within the PRACK response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
3	Security-Server	[48] 2	Х	Х	[48] 2	c1	c1		
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
c1:	IF A.4/37 THEN m ELSE no	/a security med	hanism agre	ement for the	e session initia	ation protoco)		

Prerequisite: A.6/34 - - 484 (Address Incomplete)

Table A.103: Supported headers within the PRACK response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Table A.104: Void

A.2.1.4.11 REFER method

Prerequisite A.5/16 - - REFER request

Table A.105: Supported headers within the REFER request

Item	Header		Sending		Receiving			
		Ref.	Ref. RFC Profile			RFC	Profile	
			status	status		status	status	
0A	Accept	[26] 20.1	0	0	[26] 20.1	m	m	
0B	Accept-Encoding	[26] 20.2	0	0	[26] 20.2	m	m	
1	Accept-Language	[26] 20.3	0	0	[26] 20.3	m	m	
1A	Allow	[26] 20.5	0	0	[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	0	0	[26] 20.11	m	m	
5B	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m	
5C	Content-Language	[26] 20.13	0	0	[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	0	0	[26] 20.19	0	0	
11	From	[26] 20.20	m	m	[26] 20.20	m	m	
12	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a	
13	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m	
14	Organization	[26] 20.25	0	0	[26] 20.25	0	0	
14A	P-Access-Network-Info	[52] 4.4	c12	c13	[52] 4.4	c12	c14	
14B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	с8	c8	
14C	P-Called-Party-ID	[52] 4.2	Х	Х	[52] 4.2	c10	c10	
14D	P-Charging-Function- Addresses	[52] 4.5	c17	c18	[52] 4.5	c17	c18	
14E	P-Charging-Vector	[52] 4.6	c15	c16	[52] 4.6	c15	c16	
14F	P-Preferred-Identity	[34] 9.2	с8	с7	[34] 9.2	n/a	n/a	
14G	P-Visited-Network-ID	[52] 4.3	x (note 1)	Х	[52] 4.3	c11	n/a	
14H	Privacy	[33] 4.2	c9	с9	[33] 4.2	с9	с9	
15	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a	
16	Proxy-Require	[26] 20.29	0	n/a	[26] 20.29	n/a	n/a	
17	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	m	m	
18	Refer-To	[36] 3	m	m	[36] 3	m	m	
19	Require	[26] 20.32	0	0	[26] 20.32	m	m	
20	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a	
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	Subject	[26] 20.36	0	0	[26] 20.36	0	0	
21	Supported	[26]	0	0	[26]	m	m	
		20.37,			20.37,		1	
		[26] 7.1			[26] 7.1			
22	Timestamp	[26] 20.38	с6	c6	[26] 20.38	m	m	
23	То	[26] 20.39	m	m	[26] 20.39	m	m	
24	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0	
25	Via	[26] 20.42	m	m	[26] 20.42	m	m	

IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. c1: c2: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. 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.4/8A THEN m ELSE n/a - - authentication between UA and proxy. c5: IF A.4/6 THEN o ELSE n/a - - timestamping of requests. c6: 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. IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted c8: identity within trusted networks. c9: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP). 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: c13: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. 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 c14: 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. 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 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 2). c19: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. c20: NOTE 1: The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT. 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].

Table A.106: Void

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/1 - - 100 (Trying)

Table A.107: Supported headers within the REFER response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m	
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m	
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m	
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m	
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m	
6	То	[26] 20.39	n/a	n/a	[26] 20.39	m	m	
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m	

Prerequisite A.5/17 - - REFER response

Table A.108: Supported headers within the REFER response - all remaining status-codes

Item	Header	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	
1A	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m	
2	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m	
3	Content-Language	[26] 20.13	0	0	[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	
9	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m	
10	Organization	[26] 20.25	0	0	[26] 20.25	0	0	
10A	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	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	c10	c11	[52] 4.5	c10	c11	
10D	P-Charging-Vector	[52] 4.6	с8	с9	[52] 4.6	с8	с9	
10E	P-Preferred-Identity	[34] 9.2	c3	х	[34] 9.2	n/a	n/a	
10F	Privacy	[33] 4.2	c4	c4	[33] 4.2	c4	c4	
10G	Require	[26] 20.32	m	m	[26] 20.32	m	m	
10H	Server	[26] 20.35	0	0	[26] 20.35	0	0	
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2	
12	То	[26] 20.39	m	m	[26] 20.39	m	m	
12A	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0	
13	Via	[26] 20.42	m	m	[26] 20.42	m	m	
14	Warning	[26] 20.43	o (note)	0	[26] 20.43	0	0	
c1:	IF A.4/11 THEN o ELSE n/a i	nsertion of da	ate in reques	ts and respo	nses.			
c2:	IF A.4/6 THEN m ELSE n/a ti			·				
c3:	IF A.4/25 THEN o ELSE n/a p identity within trusted networks.	orivate extens	sions to the S	Session Initia	tion Protocol	(SIP) for ass	serted	
c4:	IF A.4/26 THEN o ELSE n/a a					col (SIP).		
c5:	IF A.4/34 THEN o ELSE n/a t	he P-Access	-Network-Inf	o header exte	ension.	•		
c6:	IF A.4/34 AND A.3/1 THEN m E							
c7:	IF A.4/34 AND (A.3/7A OR A.3/7 AS acting as terminating UA or A				s-Network-In	fo header ex	tension and	
c8:	IF A.4/36 THEN o ELSE n/a t				on.			
c9:	IF A.4/36 THEN m ELSE n/a							
c10:	IF A.4/35 THEN o ELSE n/a t					on.		
-44.	IE A 4/OF THEN IN ELOF IN /o							

Prerequisite A.5/17 - - REFER response

c11:

NOTE:

Prerequisite: A.6/7 - - 202 (Accepted)

Table A.109: Supported headers within the REFER response

For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.

IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.

Item	Header	Sending			Receiving					
		Ref.	RFC	Profile	Ref.	RFC	Profile			
			status	status		status	status			
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m			
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			
5	Record-Route	[26] 20.30	m	m	[26] 20.30	m	m			
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 a	IF A.4/7 THEN m ELSE n/a authentication between UA and UA.								

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 (Ambiguous)

Table A.110: Supported headers within the REFER response

Item	Header	Sending Receiving					
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m
2	Contact	[26] 20.10	o (note)	0	[26] 20.10	m	m
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
NOTE:	The strength of this requirement	is RECOMM	ENDED rath	ner than OPT	IONAL.		

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.111: Supported headers within the REFER response

Item	Header		Sending	Sending		Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1	
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
10	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m	
c1:	IF A.5/7 THEN m ELSE n/a s	upport of aut	hentication b	etween UA a	nd 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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.112: Supported headers within the REFER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
6	Retry-After	[26] 20.33	0	0	[26] 20.33	0	0	
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/18 - - 405 (Method Not Allowed)

Table A.113: Supported headers within the REFER response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
2	Allow	[26] 20.5	m	m	[26] 20.5	m	m	
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite: A.6/20 - - 407 (Proxy Authentication Required)

Table A.114: Supported headers within the REFER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
	All	[00] 00 F			[00] 00 5			
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1	
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
8	WWW-Authenticate	[26] 20.44	0	0	[26] 20.44	0	0	
c1:	IF A.5/7 THEN m ELSE n/a s	support of aut	hentication b	etween UA a	nd UA.	•		

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/25 - - 415 (Unsupported Media Type)

Table A.115: Supported headers within the REFER response

Item	Header		Sending		Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Accept	[26] 20.1	0.1	0.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	0.1	0.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	0.1	[26] 20.3	m	m
3A	Allow	[26] 20.5	0	0	[26] 20.5	m	m
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m
0.1	At least one of these capabilities	s is supported	d.				

Prerequisite A.5/17 - - REFER response

Prerequisite: A.6/27 - - 420 (Bad Extension)

Table A.116: Supported headers within the REFER response

Item	Header		Sending		Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
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 - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.116A: Supported headers within the REFER response

Item	Header	Sending					Receiving	
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
3	Security-Server	[48] 2	Х	Х	[48] 2	c1	c1	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
c1:	IF A.4/37 THEN m ELSE n/a	security med	hanism agre	ement for the	e session initia	ation protoco	İ.	

Prerequisite: A.6/34 - - 484 (Address Incomplete)

Table A.117: Supported headers within the REFER response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Table A.118: Void

A.2.1.4.12 REGISTER method

Prerequisite A.5/18 - - REGISTER request

Table A.119: Supported headers within the REGISTER request

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Accept	[26] 20.1	0	0	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	0	0	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	0	0	[26] 20.3	m	m
3A	Allow	[26] 20.5	0	0	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c1	c1	[28] 7.2.2	c1	c1
5	Authorization	[26] 20.7, [49]	c2	c29	[26] 20.7, [49]	m	c22
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	0	0	[26] 20.9	0	0
8	Contact	[26] 20.10	0	m	[26] 20.10	m	m
9	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m
10	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m
11	Content-Language	[26] 20.13	0	0	[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	0	0	[26] 20.19	m	m
17	From	[26] 20.20	m	m	[26] 20.20	m	m
18	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
19	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m
20	Organization	[26] 20.25	0	0	[26] 20.25	0	0
20A	P-Access-Network-Info	[52] 4.4	c12	c13	[52] 4.4	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
20D	P-Visited-Network-ID	[52] 4.3	x (note 2)	Х	[52] 4.3	c10	c11
20E	Path	[35] 4	c4	c5	[35] 4	m	c6
20F	Privacy	[33] 4.2	с9	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	0	o (note 1)	[26] 20.29	n/a	n/a
23	Require	[26] 20.32	0	0	[26] 20.32	m	m
24	Route	[26] 20.34	0	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
25	Supported	[26] 20.37	0	c23	[26] 20.37	m	m
26	Timestamp	[26] 20.38	с7	с7	[26] 20.38	с7	c7
27	То	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0
29	Via	[26] 20.42	m	m	[26] 20.42	m	m

- IF A.4/20 THEN m ELSE n/a - SIP specific event notification extension. c1:
- IF A.4/8 THEN m ELSE n/a - authentication between UA and registrar. c2:
- IF A.4/11 THEN o ELSE n/a - insertion of date in requests and responses. c3:
- c4: IF A.4/24 THEN o ELSE n/a - - session initiation protocol extension header field for registering non-adjacent
- IF A.4/24 THEN x ELSE n/a - session initiation protocol extension header field for registering non-adjacent c5: contacts.
- IF A.3/4 THEN m ELSE n/a. - S-CSCF. c6:
- IF A.4/6 THEN m ELSE n/a - timestamping of requests. c7:
- IF A.4/8A THEN m ELSE n/a - authentication between UA and proxy. c8:
- IF A.4/26 THEN o ELSE n/a - a privacy mechanism for the Session Initiation Protocol (SIP). IF A.4/33 THEN o ELSE n/a - the P-Visited-Network-ID extension. c9:
- c10:
- IF A.4/33 THEN m 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:
- 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 (note 4).
- 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.
- IF A.4/36 THEN o ELSE n/a - the P-Charging-Vector header extension. c15:
- IF A.4/36 OR A.3/4 THEN m ELSE n/a - the P-Charging-Vector header extension (including S-CSCF as c16:
- IF A.4/35 THEN o ELSE n/a - the P-Charging-Function-Addresses header extension. c17:
- IF A.4/35 OR A.3/4 THEN m ELSE n/a - the P-Charging-Function-Addresses header extension (including c18: S-CSCF as registrar).
- IF A.4/37 THEN o ELSE n/a - security mechanism agreement for the session initiation protocol (note 3). c19:
- IF A.4/37 THEN m ELSE n/a - security mechanism agreement for the session initiation protocol. c20:
- IF A.4/37 AND A.4/2 THEN m ELSE n/a - security mechanism agreement for the session initiation protocol c21: and registrar.
- c22: IF A.3/4 THEN m ELSE n/a - - S-CSCF.
- IF A.3/1 THEN m ELSE o - UE. c23:
- 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.
- The strength of this requirement in RFC 3455 [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.
- NOTE 4: Refere to subclause 5.1.1.2 for information on when the UE sets the P-Access-Network-Info header.

Table A.120: Void

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/1 - - 100 (Trying)

Table A.121: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Call-ID	[26] 20.8	n/a	n/a	[26] 20.8	m	m	
2	Content-Length	[26] 20.14	n/a	n/a	[26] 20.14	m	m	
3	Cseq	[26] 20.16	n/a	n/a	[26] 20.16	m	m	
4	Date	[26] 20.17	n/a	n/a	[26] 20.17	m	m	
5	From	[26] 20.20	n/a	n/a	[26] 20.20	m	m	
6	То	[26] 20.39	n/a	n/a	[26] 20.39	m	m	
7	Via	[26] 20.42	n/a	n/a	[26] 20.42	m	m	

Table A.122: Supported headers within the REGISTER response - all status-codes

Item	Header		Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m		
1A	Call-Info	[26] 20.9	0	0	[26] 20.9	0	0		
2	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m		
3	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m		
4	Content-Language	[26] 20.13	0	0	[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	0	0	[26] 20.24	m	m		
11	Organization	[26] 20.25	0	0	[26] 20.25	0	0		
11A	P-Access-Network-Info	[52] 4.4	c3	n/a	[52] 4.4	c3	n/a		
11B	P-Charging-Function-	[52] 4.5	c6	c7	[52] 4.5	c6	c7		
	Addresses								
11C	P-Charging-Vector	[52] 4.6	c4	c5	[52] 4.6	c4	c5		
11D	Privacy	[33] 4.2	c2	n/a	[33] 4.2	c2	n/a		
11E	Require	[26] 20.32	m	m	[26] 20.32	m	m		
11F	Server	[26] 20.35	0	0	[26] 20.35	0	0		
12	Timestamp	[26] 20.38	c2	c2	[26] 20.38	m	m		
13	То	[26] 20.39	m	m	[26] 20.39	m	m		
13A	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0		
14	Via	[26] 20.42	m	m	[26] 20.42	m	m		
15	Warning	[26] 20.43	o (note)	0	[26] 20.43	0	0		
c1:	IF A.4/11 THEN o ELSE n/a	insertion of da	ate in reques	sts and respo	nses.				
c2:	IF A.4/26 THEN o ELSE n/a	a privacy med	chanism for t	he Session I	nitiation Proto	col (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 EL registrar).					(including S	CSCF as		
c6·	IF A 1/35 THEN A ELSE n/a	the P-Chargin	a-Function-	Addrassas ha	ander extensi	on			

c6:

NOTE:

IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
IF A.4/35 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension (including c7: S-CSCF as registrar).

For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.

Prerequisite: A.6/6 - - 2xx

Table A.123: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Accept	[26] 20.1	0		[26] 20.1	0		
1A	Accept-Encoding	[26] 20.2	0	0	[26] 20.2	m	m	
1B	Accept-Language	[26] 20.3	0	0	[26] 20.3	m	m	
2	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
3	Authentication-Info	[26] 20.6	с6	c6	[26] 20.6	с7	c7	
5	Contact	[26] 20.10	0	0	[26] 20.10	m	m	
5A	P-Associated-URI	[52] 4.1	с8	с9	[52] 4.1	c10	c11	
6	Path	[35] 4	c3	c3	[35] 4	c4	c4	
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 E	LSE n/a S	S-CSCF actir	ng as registra	r.			
c2:	IF A.3/4 OR A.3/1THEN m ELSI	E n/a S-C	SCF or UE.					
c3:	IF A.4/24 THEN m ELSE n/a	session initia	tion protocol	extension he	eader field for	registering r	non-	
	adjacent contacts.							
c4:	IF A.4/24 THEN o ELSE n/a s	session initiat	tion protocol	extension he	ader field for	registering n	on-adjacent	
	contacts.							
c5:	IF A.4/28 THEN m ELSE n/a	session initia	ition protocol	extension he	eader field for	service rout	e 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-Assocated-URI header extension and registrar.

c9: IF A.3/1 AND A.4/31 THEN m ELSE n/a - - P-Assocated-URI header extension and S-CSCF.

c10: IF A.4/31 THEN o ELSE n/a - - P-Assocated-URI header extension.

c11: IF A.4/31 AND A.3/1 THEN m ELSE n/a - - P-Assocated-URI header extension and UE.

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 (Ambiguous)

Table A.124: Supported headers within the REGISTER response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
3	Contact	[26] 20.10	o (note)	0	[26] 20.10	m	m		
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.								

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.125: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Proxy-Authenticate	[26] 20.27	c1	Х	[26] 20.27	c1	Х	
6	Security-Server	[48] 2	Х	Х	[48] 2	n/a	c2	
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
10	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m	
c1:	IF A.5/8 THEN m ELSE n/a support of authentication between UA and UA.							
c2:	IF A.4/37 THEN m ELSE n/a	security med	hanism agre	ement for the	e session initia	ation protoco	ol.	

Prerequisite A.5/19 - - REGISTER response

 $Prerequisite: A.6/17 \ OR \ A.6/23 \ OR \ A.6/30 \ OR \ A.6/36 \ OR \ A.6/42 \ OR \ A.6/45 \ OR \ A.6/50 \ OR \ A.6/51 \ -- \ 404, \ 413, \ 480, \ A.6/30 \ OR \ A.6/30$

486, 500, 503, 600, 603

Table A.126: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
6	Retry-After	[26] 20.33	0	0	[26] 20.33	0	0	
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/18 - - 405 (Method Not Allowed)

Table A.127: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
			อเลเนอ	อเลเนอ		อเลเนอ	อเลเนอ	
2	Allow	[26] 20.5	m	m	[26] 20.5	m	m	
4	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/20 - - 407 (Proxy Authentication Required)

Table A.128: Supported headers within the REGISTER response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
5	Proxy-Authenticate	[26] 20.27	c1	Х	[26] 20.27	c1	Х		
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
9	WWW-Authenticate	[26] 20.44	0	0	[26] 20.44	0	0		
c1·	IF A 5/8 THEN m FLSE n/a	support of aut	hentication h	etween IIA a	and LIA				

Prerequisite: A.6/25 - - 415 (Unsupported Media Type)

Table A.129: Supported headers within the REGISTER response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Accept	[26] 20.1	0.1	0.1	[26] 20.1	m	m	
2	Accept-Encoding	[26] 20.2	0.1	0.1	[26] 20.2	m	m	
3	Accept-Language	[26] 20.3	0.1	0.1	[26] 20.3	m	m	
4	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
5	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
0.1	At least one of these capabilit	ies is supported	d.					

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/27 - - 420 (Bad Extension)

Table A.130: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
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 - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.130A: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
3	Security-Server	[48] 2	c2	c2	[48] 2	c1	c1	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
c1:	IF A.4/37 THEN m ELSE n/a	security med	hanism agre	ement for the	session initia	ation protoco	l.	
c2:	IF A.4/37 AND A.4/2 THEN m E and registrar.	LSE n/a s	ecurity mech	anism agreer	ment for the s	session initiat	ion protocol	

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/29 - - 423 (Interval Too Brief)

Table A.131: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
3	Error-Info	[26] 20.18	0		[26] 20.18	0		
5	Min-Expires	[26] 20.23	m	m	[26] 20.23	m	m	
8	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite: A.6/34 - - 484 (Address Incomplete)

Table A.132: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Table A.133: Void

A.2.1.4.13 SUBSCRIBE method

Prerequisite A.5/20 - - SUBSCRIBE request

Table A.134: Supported headers within the SUBSCRIBE request

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Accept	[26] 20.1	0	0	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	0	0	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	0	0	[26] 20.3	m	m
3A	Allow	[26] 20.5	0	0	[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	Contact	[26] 20.10	m	m	[26] 20.10	m	m
7	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m
8	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m
9	Content-Language	[26] 20.13	0	0	[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
16	From	[26] 20.20	m	m	[26] 20.20	m	m
17	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
18	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m
18A	Organization	[26] 20.25	0	0	[26] 20.25	0	0
18B	P-Access-Network-Info	[52] 4.4	c12	c13	[52] 4.4	c12	c14
18C	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c6	c6
18D	P-Called-Party-ID	[52] 4.2	Х	Х	[52] 4.2	c10	c10
18E	P-Charging-Function- Addresses	[52] 4.5	c17	c18	[52] 4.5	c17	c18
18F	P-Charging-Vector	[52] 4.6	c15	c16	[52] 4.6	c15	c16
18G	P-Preferred-Identity	[34] 9.2	c6	c7	[34] 9.2	n/a	n/a
18H	P-Visited-Network-ID	[52] 4.3	x (note 2)	х	[52] 4.3	c11	n/a
181	Privacy	[33] 4.2	c9	с9	[33] 4.2	с9	c9
19	Proxy-Authorization	[26] 20.28	c5	c5	[26] 20.28	n/a	n/a
20	Proxy-Require	[26] 20.29	0	n/a	[26] 20.29	n/a	n/a
21	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	m	m
22	Require	[26] 20.32	0	0	[26] 20.32	m	m
23	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
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
24	Supported	[26] 20.37	0	0	[26] 20.37	m	m
25	Timestamp	[26] 20.38	с8	с8	[26] 20.38	m	m
26	То	[26] 20.39	m	m	[26] 20.39	m	m
27	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0
28	Via	[26] 20.42	m	m	[26] 20.42	m	m

defined by 3GPP TS 33.203 [19].

IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension. c1: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension. 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.4/8A THEN m ELSE n/a - - authentication between UA and proxy. c5: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted c6: identity within trusted networks. 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. 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). IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension. c9: 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: c13: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE. 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 c14: 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. 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 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 3). c19: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. c20: NOTE 1: The strength of this requirement is RECOMMENDED rather than OPTIONAL. The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT. Support of this header in this method is dependent on the security mechanism and the security architecture NOTE 3: which is implemented. Use of this header in this method is not appropriate to the security mechanism

Receiving

Table A.135: Void

Prerequisite A.5/21 - - SUBSCRIBE response

Header

Item

Table A.136: Supported headers within the SUBSCRIBE response - all status-codes

Sending

		Ref.	RFC	Profile	Ref.	RFC	Profile			
		i.c.i.	status	status	i.c.i.	status	status			
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m			
2	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m			
3	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m			
4	Content-Language	[26] 20.13	0	0	[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	0	0	[26] 20.24	m	m			
10A	Organization	[26] 20.25	0	0	[26] 20.25	0	0			
10B	P-Access-Network-Info	[52] 4.4	c5	c6	[52] 4.4	c5	c7			
10C	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c3	c3			
10D	P-Charging-Function-	[52] 4.5	c10	c11	[52] 4.5	c10	c11			
	Addresses									
10E	P-Charging-Vector	[52] 4.6	с8	с9	[52] 4.6	c8	с9			
10F	P-Preferred-Identity	[34] 9.2	с3	х	[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			
101	Server	[26] 20.35	0	0	[26] 20.35	0	0			
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2			
12	То	[26] 20.39	m	m	[26] 20.39	m	m			
12A	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0			
13	Via	[26] 20.42	m	m	[26] 20.42	m	m			
14	Warning	[26] 20.43	o (note)	0	[26] 20.43	0	0			
c1:	IF A.4/11 THEN o ELSE n/a i	nsertion of d	ate in reques	ts and respor	nses.					
c2:	IF A.4/6 THEN m ELSE n/a ti									
c3:	IF A.4/25 THEN o ELSE n/a p	orivate extens	sions to the S	Session Initiat	tion Protocol	(SIP) for ass	erted			
	identity within trusted networks.									
c4:	IF A.4/26 THEN o ELSE n/a a					col (SIP).				
c5:	IF A.4/34 THEN o ELSE n/a t						_			
c6:	IF A.4/34 AND A.3/1 THEN m E									
c7:	IF A.4/34 AND (A.3/7A OR A.3/7				s-Network-In	to header ext	ension and			
-0.	AS acting as terminating UA or A				_					
c8:	IF A.4/36 THEN 0 ELSE n/a t									
c9: c10:	IF A.4/36 THEN m ELSE n/a IF A.4/35 THEN o ELSE n/a t	the P-Chargi	ng-vector he	ader extensi	UII. Jodan aytansi	on				
c10:										
VIII.	IF A.4/35 THEN m ELSE n/a the P-Charging-Function-Addresses header extension.									

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/6 and A.6/7 - - 2xx

NOTE:

Table A.137: Supported headers within the SUBSCRIBE response

For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.

Item	Header			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	0	0	[26] 20.5	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
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.

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 (Ambiguous)

Table A.138: Supported headers within the SUBSCRIBE response

Item	Header		Sending		Receiving						
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status				
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m				
1	Contact	[26] 20.10	m (note)	m	[26] 20.10	m	m				
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0				
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m				
NOTE:	The strength of this requirement	The strength of this requirement is RECOMMENDED rather than MANDATORY for a 485 response.									

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.139: Supported headers within the SUBSCRIBE response

Item	Header	Sending				Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status			
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m			
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0			
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1			
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m			
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m			
c1:	IF A.5/7 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.6/50 OR A.6/51 - - 404, 413, 480, 486, 500,

600, 603

Table A.140: Supported headers within the SUBSCRIBE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
3	Retry-After	[26] 20.33	0		[26] 20.33	0		
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/18 - - 405 (Method Not Allowed)

Table A.141: Supported headers within the SUBSCRIBE response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	m	m	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/20 - - 407 (Proxy Authentication Required)

Table A.142: Supported headers within the SUBSCRIBE response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
2	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1		
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
6	WWW-Authenticate	[26] 20.44	0	0	[26] 20.44	0	0		
c1:	IF A.5/7 THEN m ELSE n/a s	support of aut	hentication b	etween UA a	and UA.	•	•		

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite A.6/25 - - 415 (Unsupported Media Type)

Table A.143: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Accept	[26] 20.1	0.1	0.1	[26] 20.1	m	m	
2	Accept-Encoding	[26] 20.2	0.1	0.1	[26] 20.2	m	m	
3	Accept-Language	[26] 20.3	o.1	0.1	[26] 20.3	m	m	
4	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
6	Server	[26] 20.35	0	0	[26] 20.35	0	0	
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
0.1	At least one of these capabilities	s is supported	d.			•		

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/27 - - 420 (Bad Extension)

Table A.144: Supported headers within the SUBSCRIBE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
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 - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.144A: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
3	Security-Server	[48] 2	Х	Х	[48] 2	c1	c1		
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
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 - - 423 (Interval Too Brief)

Table A.145: Supported headers within the SUBSCRIBE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
2	Min-Expires	[26] 20.23	m	m	[26] 20.23	m	m	
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/34 - - 484 (Address Incomplete)

Table A.146: Supported headers within the SUBSCRIBE response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/39 - - 489 (Bad Event)

Table A.147: Supported headers within the SUBSCRIBE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
1	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	m	m	
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	

Prerequisite A.5/21 - - SUBSCRIBE response

Prerequisite: A.6/45 - - 503 (Service Unavailable)

Table A.148: Supported headers within the SUBSCRIBE response

Item	Header		Sending				Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status			
0A	Allow	[26] 20.5	0	0	[26] 20.5	m	m			
1	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0			
3	Retry-After	[26] 20.33	0	0	[26] 20.33	0	m			
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m			

Table A.149: Void

A.2.1.4.14 **UPDATE** method

Prerequisite A.5/22 - - UPDATE request

Table A.150: Supported headers within the UPDATE request

Item	Header		Sending			Receiving			
1.0	l loade.	Ref.	RFC	Profile	Ref.	RFC	Profile		
		1.0	status	status	11011	status	status		
1	Accept	[26] 20.1	0	0	[26] 20.1	m	m		
2	Accept-Encoding	[26] 20.2	0	0	[26] 20.2	m	m		
3	Accept-Language	[26] 20.3	0	0	[26] 20.3	m	m		
4	Allow	[26] 20.5	0	0	[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	0	0	[26] 20.9	0	0		
9	Contact	[26] 20.10	m	m	[26] 20.10	m	m		
10	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m		
11	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m		
12	Content-Language	[26] 20.13	0	0	[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		
17	From	[26] 20.20	m	m	[26] 20.20	m	m		
18	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a		
19	MIME-Version	[26] 20.24	0	0	[26] 20.24	m	m		
20	Organization	[26] 20.25	0	0	[26] 20.25	0	0		
20A	P-Access-Network-Info	[52] 4.4	c11	c12	[52] 4.4	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		
20D	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	0	n/a	[26] 20.29	n/a	n/a		
23	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	n/a	n/a		
24	Require	[26] 20.32	0	0	[26] 20.32	m	m		
25	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a		
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		
26	Supported	[26] 20.37	0	0	[26] 20.37	m	m		
27	Timestamp	[26] 20.38	с9	с9	[26] 20.38	m	m		
28	То	[26] 20.39	m	m	[26] 20.39	m	m		
29	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0		
30	Via	[26] 20.42	m	m	[26] 20.42	m	m		
c2:	IF A.4/20 THEN 0 ELSE n/a								
c3:	IF A.4/20 THEN m ELSE n/a				n.				
c4:	IF A.4/7 THEN m ELSE n/a a								
c5:	IF A.4/11 THEN 0 ELSE n/a					aal (CID)			
c6:	IF A.4/26 THEN o ELSE n/a til			ne Session ii	illiation Proto	icoi (SIP).			
c9:				IA and provi					
c10: c11:	IF A.4/8A THEN m ELSE n/a								
c12:	IF A.4/34 THEN o ELSE n/a the P-Access-Network-Info header extension. 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) 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.								
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								
c18:	IF A.4/37 THEN 0 ELSE n/a :								
c19:	IF A.4/37 THEN m ELSE n/a	security med	nanısm agre	ement for the	e session initia	ation protoco	DI.		

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].

Table A.151: Void

Prerequisite A.5/23 - - UPDATE response

Table A.152: Supported headers within the UPDATE response - all remaining status-codes

Item	Header	Sending Receiving						
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m	
1A	Call-Info	[26] 20.9	0	0	[26] 20.9	0	0	
2	Content-Disposition	[26] 20.11	0	0	[26] 20.11	m	m	
3	Content-Encoding	[26] 20.12	0	0	[26] 20.12	m	m	
4	Content-Language	[26] 20.13	0	0	[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	0	0	[26] 20.24	m	m	
10A	Organization	[26] 20.25	0	0	[26] 20.25	0	0	
10B	P-Access-Network-Info	[52] 4.4	c4	c5	[52] 4.4	c4	c6	
10C	P-Charging-Function-	[52] 4.5	с9	c10	[52] 4.5	с9	c10	
	Addresses							
10D	P-Charging-Vector	[52] 4.6	c7	c8	[52] 4.6	c7	c8	
10E	Privacy	[33] 4.2	c3	n/a	[33] 4.2	c3	n/a	
10F	Require	[26] 20.31	m	m	[26] 20.31	m	m	
10G	Server	[26] 20.35	0	0	[26] 20.35	0	0	
11	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2	
12	То	[26] 20.39	m	m	[26] 20.39	m	m	
12A	User-Agent	[26] 20.41	0	0	[26] 20.41	0	0	
13	Via	[26] 20.42	m	m	[26] 20.42	m	m	
14	Warning	[26] 20.43	o (note)	0	[26] 20.43	0	0	
c1:	IF A.4/11 THEN o ELSE n/a i	nsertion of da	ate in reques	ts and respor	nses.			
c2:	IF A.4/6 THEN m ELSE n/a ti							
c3:	IF A.4/26 THEN o ELSE n/a a	a privacy med	chanism for t	he Session Ir	nitiation Proto	col (SIP).		
c4:	IF A.4/34 THEN o ELSE n/a t							
c5:	IF A.4/34 AND A.3/1 THEN m E							
c6:	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.							
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							
c9:	IF A.4/35 THEN o ELSE n/a t							
c10:	IF A.4/35 THEN m ELSE n/a							

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/6 - - 2xx

Table A.153: Supported headers within the UPDATE response

NOTE: For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
0A	Accept	[26] 20.1	0	0	[26] 20.1	m	m	
0B	Accept-Encoding	[26] 20.2	0	0	[26] 20.2	m	m	
0C	Accept-Language	[26] 20.3	0	0	[26] 20.3	m	m	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
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	
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
c1: c2:	IF A.4/7 THEN o ELSE n/a authentication between UA and UA. IF A.4/7 THEN m ELSE n/a authentication between UA and UA.							

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 - - 3xx

Table A.154: Supported headers within the UPDATE response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Contact	[26] 20.10	0	0	[26] 20.10	0	0	
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.154A: Supported headers within the UPDATE response

Item	Header		Sending			Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status			
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m			
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0			
3	Proxy-Authenticate	[26] 20.27	0		[26] 20.27	0				
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m			
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m			
c1:	c1: IF A.5/7 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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.155: Supported headers within the UPDATE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
5	Retry-After	[26] 20.33	0	0	[26] 20.33	0	0	
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/18 - - 405 (Method Not Allowed)

Table A.156: Supported headers within the UPDATE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	m	m	
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m	

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/20 - - 407 (Proxy Authentication Required)

Table A.157: Supported headers within the UPDATE response

Item	Header		Sending		Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
	All	[00] 00 F			[00] 00 5				
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
4	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1		
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
8	WWW-Authenticate	[26] 20.44	0	0	[26] 20.44	0	0		
c1:	IF A.5/7 THEN m ELSE n/a support of authentication between UA and UA.								

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/25 - - 415 (Unsupported Media Type)

Table A.158: Supported headers within the UPDATE response

Item	Header		Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
1	Accept	[26] 20.1	o.1	0.1	[26] 20.1	m	m		
2	Accept-Encoding	[26] 20.2	0.1	0.1	[26] 20.2	m	m		
3	Accept-Language	[26] 20.3	0.1	0.1	[26] 20.3	m	m		
4	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
6	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
10	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
0.1	At least one of these capabilities	s is supported	d.						

Prerequisite A.5/23 - - UPDATE response

Prerequisite: A.6/27 - - 420 (Bad Extension)

Table A.159: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0
6	Supported	[26] 20.37	m	m	[26] 20.37	m	m
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 - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.159A: Supported headers within the UPDATE response

Item	Header	Sending			Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
3	Security-Server	[48] 2	Х	Х	[48] 2	c1	c1		
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
c1:	IF A.4/37 THEN m ELSE n/a	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.6/35 - - 485 (Ambiguous)

Table A.160: Supported headers within the UPDATE response

Item	Header	Sending			Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
2	Contact	[26] 20.10	o (note)	0	[26] 20.10	m	m		
3	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.								

Table A.161: Void

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
	Capabilities within main protocol			
3	initiate session release?	[26] 16	х	c27
4	stateless proxy behaviour?	[26] 16.11	o.1	c28
5	stateful proxy behaviour?	[26] 16.2	o.1	c29
6	forking of initial requests?	[26] 16.1	c1	X
7	support of TLS connections on the	[26] 16.7	0	n/a
	upstream side?			
8	support of TLS connections on the	[26] 16.7	0	n/a
	downstream side?			
8A	authentication between UA and proxy?	[26] 20.28,	0	Х
		22.3		
9	insertion of date in requests and	[26] 20.17	0	0
	responses?			
10	suppression or modification of alerting	[26] 20.4	0	0
	information data?			
11	reading the contents of the Require	[26] 20.32	0	0
	header before proxying the request or			
12	response?	[26] 20 22		
12	adding or modifying the contents of the Require header before proxying the	[26] 20.32	0	m
	REGISTER request or response			
13	adding or modifying the contents of the	[26] 20.32	0	0
13	Require header before proxying the	[20] 20.02		
	request or response for methods other			
	than REGISTER?			
14	being able to insert itself in the	[26] 16.6	0	c2
• •	subsequent transactions in a dialog	[20] :0:0		
	(record-routing)?			
15	the requirement to be able to use	[26] 16.7	c3	c3
	separate URIs in the upstream direction			
	and downstream direction when record			
	routeing?			
16	reading the contents of the Supported	[26] 20.37	0	0
	header before proxying the response?			
17	reading the contents of the	[26] 20.40	0	m
	Unsupported header before proxying			
40	the 420 response to a REGISTER?	[00] 00 40	_	_
18	reading the contents of the	[26] 20.40	0	0
	Unsupported header before proxying			
	the 420 response to a method other than REGISTER?			
19	the inclusion of the Error-Info header in	[26] 20.18	0	0
13	3xx - 6xx responses?	[20] 20.10		
19A	reading the contents of the	[26] 20.25	0	0
	Organization header before proxying	[=0] =0.=0		
	the request or response?			
19B	adding or concatenating the	[26] 20.25	0	0
	Organization header before proxying			
	the request or response?			
19C	reading the contents of the Call-Info	[26] 20.9	0	0
	header before proxying the request or			
	response?			
19D	adding or concatenating the Call-Info	[26] 20.9	0	0
	header before proxying the request or			
405	response?	[00] 00	1	1
19E	delete Contact headers from 3xx	[26] 20	0	0
	responses prior to relaying the			
	response? Extensions			
20	the SIP INFO method?	[25]	0	0
21	reliability of provisional responses in	[27]	0	i
'	Light the state of	[-']		L '

	SIP?	1		
22	the REFER method?	[36]		
23	integration of resource management and SIP?	[30]	0	i
24	the SIP UPDATE method?	[29]	c4	i
26	SIP extensions for media authorization?	[31]	0	c7
27	SIP specific event notification	[28]	0	i
28	the use of NOTIFY to establish a dialog	[28] 4.2	0	n/a
29	Session Initiation Protocol Extension	[35]	0	c6
	Header Field for Registering Non- Adjacent Contacts		Ŭ	00
30	extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks	[34]	0	m
30A	act as first entity within the trust domain for asserted identity	[34]	c5	c8
30B	act as subsequent entity within trust network that can route outside the trust network	[34]	c5	c9
31	a privacy mechanism for the Session Initiation Protocol (SIP)	[33]	0	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
32	Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration	[38]	0	c30
33	a messaging mechanism for the Session Initiation Protocol (SIP)	[50]	0	m
34	Compressing the Session Initiation Protocol	[55]	0	с7
35	private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)?	[52]	0	m
36	the P-Associated-URI header extension?	[52] 4.1	c14	c15
37	the P-Called-Party-ID header extension?	[52] 4.2	c14	c16
38	the P-Visited-Network-ID header extension?	[52] 4.3	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	c14	c19
42	act as first entity within the trust domain	[52] 4.4	c20	c21

	for access network information?			
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	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	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]	0	с7

c1:	IF A.162/5 THEN o ELSE n/a stateful proxy behaviour.
c2:	IF A.3/2 OR A.3/3A OR A.3/4 THEN m ELSE o P-CSCF, I-CSCF(THIG) or S-CSCF.
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.3/3A THEN m ELSE n/a P-CSCF or I-CSCF (THIG).
c7:	IF A.3/2 THEN m ELSE n/a P-CSCF.
c8:	IF A.3/2 AND A.162/30 THEN m ELSE n/a P-CSCF and extensions to the Session
00.	Initiation Protocol (SIP) for asserted identity within trusted networks.
c9:	IF A.3/2 AND A.162/30 THEN m ELSE IF A.3/7C AND A.162/30 THEN o ELSE n/a
65.	S-CSCF or AS acting as proxy and extensions to the Session Initiation Protocol (SIP)
	for asserted identity within trusted networks (NOTE).
c10:	IF A.162/31 THEN 0.2 ELSE n/a a privacy mechanism for the Session Initiation
610.	· · ·
-44.	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 n/a S-CSCF.
c13:	IF A.162/31 AND (A.3/2 OR A.3/3 OR A.3/7C) THEN m ELSE n/a P-CSCF OR I-
	CSCF OR AS acting as a SIP 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) 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.
c16:	IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/4) 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.
c17:	IF A.162/35 AND (A.3/2 OR A.3/3) 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.
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
0.0.	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
021.	extension and P-CSCF.
c22:	IF A.162/41 AND A.3/4 THEN m ELSE n/a the P-Access-Network-Info header
622.	extension and S-CSCF.
022.	
c23:	IF A.162/45 THEN o ELSE n/a the P-Charging-Vector header extension. IF A.162/45 THEN m ELSE n/a the P-Charging-Vector header extension.
c24:	
c25:	IF A.162/44 THEN o ELSE n/a the P-Charging-Function-Addresses header
-00:	extension.
c26:	IF A.162/44 THEN m ELSE n/a the P-Charging-Function Addresses header
-07	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.3/4 OR A.3/6 then m ELSE o P-CSCF or S-CSCF of MGCF.
c29:	IF A.3/2 OR A.3/4 OR A.3/6 then o ELSE m P-CSCF or S-CSCF of MGCF.
c30:	IF A.3/2 o ELSE i P-CSCF.
0.1:	It is mandatory to support at least one of these items.
0.2:	It is mandatory to support at least one of these items.
0.3:	It is mandatory to support at least one of these items.
NOTE:	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.

A.2.2.3 PDUs

Table A.163: Supported methods

Item	PDU		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	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
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
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	[30] 7	c4	c4	[30] 7	c4	c4
23	UPDATE response	[30] 7	c4	c4	[30] 7	c4	c4
c1:	IF A.162/22 THEN m ELSE n/a						·
c3	IF A.162/27 THEN m ELSE n/a						
c4	IF A.162/24 THEN m ELSE n/a						
c5:	IF A.162/33 THEN m ELSE n/a			thod.			
		11 1 1114					

c6: IF A.162/21 THEN m ELSE n/a - - reliability of provisional responses.

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] 21.1.1	c1	c1	[26] 21.1.1	c2	c2		
2	180 (Ringing)	[26] 21.1.2	сЗ	сЗ	[26] 21.1.2	сЗ	сЗ		
3	181 (Call Is Being Forwarded)	[26] 21.1.3	сЗ	с3	[26] 21.1.3	с3	с3		
4	182 (Queued)	[26] 21.1.4	с3	с3	[26] 21.1.4	с3	с3		
5	183 (Session Progress)	[26] 21.1.5	с3	с3	[26] 21.1.5	с3	с3		
6	200 (OK)	[26] 21.2.1			[26] 21.2.1				
7	202 (Accepted)	[28] 8.3.1	c4	c4	[28] 8.3.1	c4	c4		
8	300 (Multiple Choices)	[26] 21.3.1			[26] 21.3.1				
9	301 (Moved Permanently)	[26] 21.3.2			[26] 21.3.2				
10	302 (Moved Temporarily)	[26] 21.3.3			[26] 21.3.3				
11	305 (Use Proxy)	[26] 21.3.4			[26] 21.3.4				
12	380 (Alternative Service)	[26] 21.3.5			[26] 21.3.5				
13	400 (Bad Request)	[26] 21.4.1			[26] 21.4.1				
14	401 (Unauthorized)	[26] 21.4.2			[26] 21.4.2				
15	402 (Payment Required)	[26] 21.4.3			[26] 21.4.3				
16	403 (Forbidden)	[26] 21.4.4			[26] 21.4.4				
17	404 (Not Found)	[26] 21.4.5			[26] 21.4.5				
18	405 (Method Not Allowed)	[26] 21.4.6			[26] 21.4.6				
19	406 (Not Acceptable)	[26] 21.4.7			[26] 21.4.7				
20	407 (Proxy Authentication Required)	[26] 21.4.8			[26] 21.4.8				
21	408 (Request Timeout)	[26] 21.4.9			[26] 21.4.9				
22	410 (Gone)	[26] 21.4.10			[26] 21.4.10				
23	413 (Request Entity Too Large)	[26] 21.4.11			[26] 21.4.11				
24	414 (Request-URI Too Large)	[26] 21.4.12			[26] 21.4.12				
25	415 (Unsupported Media Type)	[26] 21.4.13			[26] 21.4.13				
26	416 (Unsupported URI Scheme)	[26] 21.4.14			[26] 21.4.14				
27	420 (Bad Extension)	[26] 21.4.15			[26] 21.4.15				
28	421 (Extension Required)	[26] 21.4.16			[26] 21.4.16				
29	423 (Interval Too Brief)	[26] 21.4.17	c5	c5	[26] 21.4.17	c6	c6		

Item	Header		Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
30	480 (Temporarily not	[26]			[26]				
	available)	21.4.18			21.4.18				
31	481 (Call /Transaction Does	[26]			[26]				
	Not Exist)	21.4.19			21.4.19				
32	482 (Loop Detected)	[26]			[26]				
		21.4.20			21.4.20				
33	483 (Too Many Hops)	[26]			[26]				
		21.4.21			21.4.21				
34	484 (Address Incomplete)	[26]			[26]				
		21.4.22			21.4.22				
35	485 (Ambiguous)	[26]			[26]				
	1.5.7.4	21.4.23			21.4.23				
36	486 (Busy Here)	[26]			[26]				
	10-10-10-10-10-10-10-10-10-10-10-10-10-1	21.4.24			21.4.24				
37	487 (Request Terminated)	[26]			[26]				
	100 (1) (1)	21.4.25			21.4.25				
38	488 (Not Acceptable Here)	[26]			[26]				
00	100 (D. 15t)	21.4.26	1		21.4.26		1		
39	489 (Bad Event)	[28] 7.3.2	c4	c4	[28] 7.3.2	c4	c4		
40	491 (Request Pending)	[26]			[26]				
	100 (11 1 1 1 1 1 1	21.4.27			21.4.27				
41	493 (Undecipherable)	[26]			[26]				
44.0	404 (Coourity Agreement	21.4.28	-7	-7	21.4.28		/		
41A	494 (Security Agreement	[48] 2	с7	c7	[48] 2	n/a	n/a		
42	Required) 500 (Internal Server Error)	[26]	<u> </u>		[26]				
42	500 (Internal Server Entity)	21.5.1			21.5.1				
43	501 (Not Implemented)	[26]			[26]				
43	301 (Not implemented)	21.5.2			21.5.2				
44	502 (Bad Gateway)	[26]			[26]				
77	302 (Bad Gateway)	21.5.3			21.5.3				
45	503 (Service Unavailable)	[26]			[26]				
.0	Cos (Corrido Criavalidado)	21.5.4			21.5.4				
46	504 (Server Time-out)	[26]			[26]				
		21.5.5			21.5.5				
47	505 (Version not supported)	[26]			[26]				
		21.5.6			21.5.6				
48	513 (Message Too Large)	[26]			[26]				
		21.5.7			21.5.7				
49	580 (Precondition Failure)	[30] 8			[30] 8				
50	600 (Busy Everywhere)	[26]			[26]				
	, , ,	21.6.1			21.6.1				
51	603 (Decline)	[26]			[26]				
		21.6.2			21.6.2				
52	604 (Does Not Exist	[26]			[26]				
	Anywhere)	21.6.3			21.6.3				
53	606 (Not Acceptable)	[26]			[26]				
		21.6.4			21.6.4				

c1:

IF A.162/15 THEN m ELSE n/a - - stateful proxy. IF A.162/15 THEN m ELSE i - - the requirement to be able to use separate URIs in the upstream direction c2: and downstream direction when record routeing.

c3:

IF A.163/9 THEN m ELSE n/a - - INVITE response. IF A.162/27 THEN m ELSE n/a - - SIP specific event notification. c4:

IF A.163/19 OR A.163/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response. IF A.163/19 OR A.163/21 THEN i ELSE n/a - - REGISTER response or SUBSCRIBE response. c5:

c6:

IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.

A.2.2.4.2 ACK method

Prerequisite A.163/1 - - ACK request

Table A.165: Supported headers within the ACK request

Item	Header		Sending			Receiving	<u></u>	
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
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	
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	
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	Privacy	[33] 4.2	c6	с6	[33] 4.2	c7	c7	
18	Require	[26] 20.32	m	m	[26] 20.32	c5	c5	
19	Route	[26] 20.34	m	m	[26] 20.34	m	m	
20	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i	
21	То	[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 SI	P specific eve	ent notification	n extension.				
c2:	IF A.162/9 THEN m ELSE i ir	nsertion of da	ite in request	s and respor	ises.			
c3:	IF A.3/2 OR A.3/4 THEN m ELS	E i P-CSC	F or S-CSC	F.				
c4:	IF A.162/8A THEN m ELSE i							
c5:	IF A.162/11 OR A.162/13 THEN							
	the request or response or adding or modifying the contents of the Require header before proxying the						ing the	
İ	request or response for method	se for methods other than REGISTER.						
c6:	IF A.162/31 THEN m ELSE n/a a privacy mechanism for the Session Initiation Protocol (SIP).							

IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).

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.

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. NOTE:

c7:

Table A.166: Void

A.2.2.4.3 BYE method

Prerequisite A.163/2 - - BYE request

Table A.167: Supported headers within the BYE request

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	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	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
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	c13	c13	[52] 4.4	c14	c14
16B	P-Asserted-Identity	[34] 9.1	с9	с9	[34] 9.1	c10	c10
16C	P-Charging-Function-	[52] 4.5	c17	c17	[52] 4.5	c18	c18
	Addresses						
16D	P-Charging-Vector	[52] 4.6	c15	n/a	[52] 4.6	c16	n/a
16E	P-Preferred-Identity	[34] 9.2	X	Х	[34] 9.2	c8	n/a
16F	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
19	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
20	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
21	Route	[26] 20.34	m	m	[26] 20.34	m	m
21A	Security-Client	[48] 2.3.1	Х	х	[48] 2.3.1	c19	c19
21B	Security-Verify	[48] 2.3.1	Х	Х	[48] 2.3.1	c19	c19
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	То	[26] 20.39	m	m	[26] 20.39	m	m
25	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
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 THEN m ELSE n/a security mechanism agreement for the session initiation protocol.
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.168: Void

Prerequisite: A.163/3 - - BYE response

Prerequisite: A.164/1 - - 100 (Trying)

Table A.169: Supported headers within the BYE response

Item	Header		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		
6	То	[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 THEN m ELSE i -	- insertion of da	ite in reques	ts and respor	nses.				

Prerequisite A.163/3 - - BYE response

Table A.170: Supported headers within the BYE response - all remaining status-codes

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
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	c12	c12	[52] 4.4	c13	c13
10B	P-Asserted-Identity	[34] 9.1	c4	c4	[34] 9.1	c5	c5
10C	P-Charging-Function- Addresses	[52] 4.5	c10	c10	[52] 4.5	c11	c11
10D	P-Charging-Vector	[52] 4.6	с8	n/a	[52] 4.6	с9	n/a
10E	P-Preferred-Identity	[34] 9.2	х	х	[34] 9.2	c3	n/a
10F	Privacy	[33] 4.2	c6	c6	[33] 4.2	с7	с7
10G	Require	[26] 20.32	m	m	[26] 20.32	c14	c14
10H	Server	[26] 20.35	m	m	[26] 20.35	i	i
11	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
12	То	[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 da	ite in reques	ts and respor	nses.		

- IF A.3/2 OR A.3/4 THEN m ELSE i - P-CSCF or S-CSCF. 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.
- 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
- IF A.162/31 THEN m ELSE n/a - a privacy mechanism for the Session Initiation Protocol (SIP). c6:
- 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.
- 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 Pc9: 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.
- IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - adding, deleting or reading the P-Chargingc11: Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
- IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - act as subsequent entity within trust network c12: for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
- IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - act as subsequent entity within trust network c13: 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.

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/6 - - 2xx

Table A.171: Supported headers within the BYE response

Item	Header	Sending				Receiving				
		Ref.	RFC	Profile	Ref.	RFC	Profile			
			status	status		status	status			
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i			
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			
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 route	ing.							

Prerequisite A.163/3 - BYE response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 (Ambiguous)

Table A.172: Supported headers within the BYE response

Item	Header		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	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1				
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i				
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i				
c1:	IF A.162/19E THEN m ELSE i -	IF A.162/19E THEN m ELSE i deleting Contact headers.									

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.173: Supported headers within the BYE response

Item	Header	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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m		
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i		
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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.174: Supported headers within the BYE response

Item	Header	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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
3	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/18 - - 405 (Method Not Allowed)

Table A.175: Supported headers within the BYE response

Item	Header	Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/20 - - 407 (Proxy Authentication Required)

Table A.176: Supported headers within the BYE response

Item	Header		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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i	

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/25 - - 415 (Unsupported Media Type)

Table A.177: Supported headers within the BYE response

Item	Header	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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/27 - - 420 (Bad Extension)

Table A.178: Supported headers within the BYE response

Item	Header		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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
							<u> </u>		
4	Supported	[26] 20.37	m	m	[26] 20.37	I	I		
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 - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.178A: Supported headers within the BYE response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
3	Security-Server	[48] 2	c1	c1	[48] 2	n/a	n/a	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
c1:	IF A.162/47 THEN m ELSE n/a	security m	echanism ac	reement for	the session ir	nitiation prote	col.	

Prerequisite A.163/3 - - BYE response

Prerequisite: A.164/34 - - 484 (Address Incomplete)

Table A.179: Supported headers within the BYE response

Item	Header	Sending			Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Table A.180: Void

A.2.2.4.4 CANCEL method

Prerequisite A.163/4 - - CANCEL request

Table A.181: Supported headers within the CANCEL request

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
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
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
12	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
13	Privacy	[33] 4.2	c3	c3	[33] 4.2	c4	c4
16	Record-Route	[26] 20.30	m	m	[26] 20.30	с7	c7
18	Route	[26] 20.34	m	m	[26] 20.34	m	m
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	То	[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 SI	P specific eve	ent notification	n extension.			
c2:	IF A.162/9 THEN m ELSE i ir				ses.		
c3:	IF A.162/31 THEN m ELSE n/a	a privacy r	mechanism f	or the Sessio	n Initiation Pi	rotocol (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						
c7:	response. IF A.162/14 THEN o ELSE i t	the requireme	ent to be able	to insert itse	elf in the subs	equent trans	actions in a

c7: IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.

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.182: Void

Prerequisite A.163/5 - - CANCEL response

Table A.183: Supported headers within the CANCEL response - all status-codes

Item	Header		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
5A	Privacy	[33] 4.2	c2	c2	[33] 4.2	c3	c3
6	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
7	То	[26] 20.39	m	m	[26] 20.39	m	m
7A	User-Agent	[26] 20.41	0		[26] 20.41	0	
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.

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/6 - - 200 (OK)

Table A.184: Supported headers within the CANCEL response

Item	Header		Sending Receiving					
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
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 t and downstream direction when			to use sepa	rate URIs in t	he upstream	direction	

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.185: Supported headers within the CANCEL response

Item	Header	Sending				Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/5 - - CANCEL response

 $Prerequisite: A.164/17 \ OR \ A.164/23 \ OR \ A.164/30 \ OR \ A.164/42 \ OR \ A.164/45 \ OR \ A.164/50 \ OR \ A.164/51 \ - \ - \ 404, \ 413, \ A.164/50 \ OR$

480, 500, 503, 600, 603

Table A.186: Supported headers within the CANCEL response

Item	Header		Sending		Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
2	Error-Info	[26] 2418	m	m	[26] 20.18	i	i
4	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/5 - - CANCEL response

Prerequisite: A.164/34 - - 484 (Address Incomplete)

Table A.188: Supported headers within the CANCEL response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Table A.189: Void

A.2.2.4.5 COMET method

Void

A.2.2.4.6 INFO method

Void

A.2.2.4.7 INVITE method

Prerequisite A.163/8 - - INVITE request

Table A.204: Supported headers within the INVITE request

Item	Header		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	T i	
3	Accept-Language	[26] 20.3	m	m	[26] 20.3	i	T 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	T i	
6	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1	
8	Authorization	[26] 20.7	m	m	[26] 20.7	i	T 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	
20	From	[26] 20.20	m	m	[26] 20.20	m	m	
21	In-Reply-To	[26] 20.21	m	m	[26] 20.21	i	i	
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	
24	Organization	[26] 20.25	m	m	[26] 20.25	c5	c5	
24A	P-Access-Network-Info	[52] 4.4	c28	c28	[52] 4.4	c29	c30	
24B	P-Asserted-Identity	[34] 9.1	c15	c15	[34] 9.1	c16	c16	
24C	P-Called-Party-ID	[52] 4.2	c19	c19	[52] 4.2	c20	c21	
24D	P-Charging-Function- Addresses	[52] 4.5	c26	c27	[52] 4.5	c26	c27	
24E	P-Charging-Vector	[52] 4.6	c24	c24	[52] 4.6	c25	c25	
25	P-Media-Authorization	[31] 6.1	с9	c10	[31] 6.1	n/a	n/a	
25A	P-Preferred-Identity	[34] 9.2	х	х	[34] 9.2	c14	c14	
25B	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	
27	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c13	c13	
28	Proxy-Require	[26] 20.29,	m	m	[26] 20.29,	m	m	
		[34] 4			[34] 4			
29	Record-Route	[26] 20.30	m	m	[26] 20.30	c11	c11	
31	Reply-To	[26] 20.31	m	m	[26] 20.31	İ	i	
32	Require	[26] 20.32	m	m	[26] 20.32	с7	c7	
33	Route	[26] 20.34	m	m	[26] 20.34	m	m	
33A	Security-Client	[48] 2.3.1	Х	Х	[48] 2.3.1	c31	c31	
33B	Security-Verify	[48] 2.3.1	х	х	[48] 2.3.1	c31	c31	
34	Subject	[26] 20.36	m	m	[26] 20.36	i	i	

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
35	Supported	[26] 20.37	m	m	[26] 20.37	с8	с8	
36	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i	
37	То	[26] 20.39	m	m	[26] 20.39	m	m	
38	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i	
39	Via	[26] 20.42	m	m	[26] 20.42	m	m	
c1:	IF A.4/20 THEN m ELSE i SI	P specific eve	ent notification	n extension.				
c2:	IF A.162/10 THEN n/a ELSE m					n data.		
c3:	IF A.162/10 THEN m ELSE i	suppression	or modificati	on of alerting	information o	lata.		
4	IE 4 400/0 THEN							

- 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.
- IF A.3/2 OR A.3/4 THEN m ELSE i - P-CSCF or S-CSCF. c6:
- 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.
- IF A.162/16 THEN m ELSE i - reading the contents of the Supported header before proxying the c8:
- c9: IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization.
- c10: IF A.3/2 THEN m ELSE n/a - - P-CSCF.
- IF A.162/14 THEN m ELSE i - the requirement to be able to insert itself in the subsequent transactions in c11:
- c12. IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
- IF A.162/8A THEN m ELSE i - authentication between UA and proxy. c13:
- IF A.162/30A THEN m ELSE n/a - act as first entity within the trust domain for asserted identity. c14:
- IF A.162/30 THEN m ELSE n/a - extensions to the Session Initiation Protocol (SIP) for asserted identity c15: within trusted networks.
- IF A.162/30A or A.162/30B THEN m ELSE i - extensions to the Session Initiation Protocol (SIP) for c16: asserted identity within trusted networks or subsequent entity within trust network that can route outside the
- c17: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
- IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - application of the privacy c18: 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.
- IF A.162/37 THEN i ELSE n/a - the P-Called-Party-ID header extension. c20:
- c21: IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND A.3/3 THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or I-CSCF.
- IF A.162/38 THEN m ELSE n/a - the P-Visited-Network-ID header extension. c22:
- IF A.162/39 THEN m ELSE i - reading, or deleting the P-Visited-Network-ID header before proxying the c23: request or response.
- IF A.162/45 THEN m ELSE n/a - the P-Charging-Vector header extension. c24:
- IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - adding, deleting, reading or modifying the Pc25: Charging-Vector header before proxying the request or response or the P-Charging-Vector header
- c26: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
- IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - adding, deleting or reading the P-Chargingc27: 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).
- IF A.162/47 THEN m ELSE n/a - security mechanism agreement for the session initiation protocol. c31:
- 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.205: Void

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/1 - - 100 (Trying)

Table A.206: Supported headers within the INVITE response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	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	То	[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.

Table A.207: Supported headers within the INVITE response - all remaining status-codes

Header		Sending		Receiving			
	Ref.	RFC	Profile	Ref.	RFC	Profile	
		status	status		status	status	
Call-ID	[26] 20.8	m	m	[26] 20.8	m	m	
Call-Info	[26] 20.9	m	m	[26] 20.9	c4	c4	
Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	c3	
Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	c3	
Content-Language	[26] 20.13	m	m	[26] 20.13	i	c3	
Content-Length	[26] 20.14	m	m	[26] 20.14	m	m	
Content-Type	[26] 20.15	m	m	[26] 20.15	i	c3	
Cseq	[26] 20.16	m	m	[26] 20.16	m	m	
Date	[26] 20.17	m	m	[26] 20.17	c1	c1	
From	[26] 20.20	m	m	[26] 20.20	m	m	
MIME-Version	[26] 20.24	m	m	[26] 20.24	i	c3	
Organization	[26] 20.25	m	m	[26] 20.25	c2	c2	
P-Access-Network-Info	[52] 4.4	c14	c14	[52] 4.4	c15	c15	
P-Asserted-Identity	[34] 9.1	c6	c6	[34] 9.1	c7	c7	
P-Charging-Function- Addresses	[52] 4.5	c12	c12	[52] 4.5	c13	c13	
P-Charging-Vector	[52] 4.6	c10	c10	[52] 4.6	c11	c11	
P-Preferred-Identity	[34] 9.2	Х	Х	[34] 9.2	c5	n/a	
Privacy	[33] 4.2	с8	c8	[33] 4.2	с9	с9	
Require	[26] 20.32	m	m	[26] 20.32	c16	c16	
Server	[26] 20.35	m	m	[26] 20.35	i	i	
Timestamp	[26] 20.38	m	m	[26] 20.38	i	i	
То	[26] 20.39	m	m	[26] 20.39	m	m	
User-Agent	[26] 20.41	m	m	[26] 20.41	i	i	
Via	[26] 20.42	m	m	[26] 20.42	m	m	
Warning	[26] 20.43	m	m	[26] 20.43	i	i	
IF A.162/9 THEN m ELSE i	insertion of da	te in request	ts and respor	ises.			
	Call-ID Call-Info Content-Disposition Content-Encoding Content-Language Content-Length Content-Type Cseq Date From MIME-Version Organization P-Access-Network-Info P-Asserted-Identity P-Charging-Function-Addresses P-Charging-Vector P-Preferred-Identity Privacy Require Server Timestamp To User-Agent Via Warning	Call-ID [26] 20.8 Call-Info [26] 20.9 Content-Disposition [26] 20.11 Content-Encoding [26] 20.12 Content-Language [26] 20.13 Content-Length [26] 20.14 Content-Type [26] 20.15 Cseq [26] 20.15 Date [26] 20.17 From [26] 20.20 MIME-Version [26] 20.24 Organization [26] 20.25 P-Access-Network-Info [52] 4.4 P-Asserted-Identity [34] 9.1 P-Charging-Function-Addresses [52] 4.5 P-Charging-Vector [52] 4.6 P-Preferred-Identity [34] 9.2 Privacy [33] 4.2 Require [26] 20.32 Server [26] 20.35 Timestamp [26] 20.38 To [26] 20.39 User-Agent [26] 20.41 Via [26] 20.42 Warning [26] 20.43	Ref. RFC status	Ref. RFC status status	Ref. RFC status Profile status Ref. Call-ID [26] 20.8 m m [26] 20.8 Call-Info [26] 20.9 m m [26] 20.9 Content-Disposition [26] 20.11 m m [26] 20.11 Content-Encoding [26] 20.12 m m [26] 20.12 Content-Language [26] 20.13 m m [26] 20.13 Content-Length [26] 20.14 m m [26] 20.13 Content-Type [26] 20.15 m m [26] 20.14 Content-Type [26] 20.15 m m [26] 20.15 Cseq [26] 20.15 m m [26] 20.15 Content-Type [26] 20.15 m m [26] 20.15 Content-Type [26] 20.16 m m [26] 20.15 Cseq [26] 20.17 m m [26] 20.15 Cseq [26] 20.17 m m [26] 20.20 MIME-Version [26] 20.24 m<	Ref. RFC status Profile status Ref. RFC status Call-ID [26] 20.8 m m [26] 20.8 m Call-Info [26] 20.9 m m [26] 20.9 c4 Content-Disposition [26] 20.11 m m [26] 20.11 i Content-Encoding [26] 20.12 m m [26] 20.12 i Content-Language [26] 20.13 m m [26] 20.13 i Content-Length [26] 20.14 m m [26] 20.15 i Content-Type [26] 20.15 m m [26] 20.15 i Cseq [26] 20.15 m m [26] 20.15 i Cseq [26] 20.16 m m [26] 20.16 m Date [26] 20.17 m m [26] 20.17 c1 From [26] 20.20 m m [26] 20.20 m MIME-Version [26] 20.24 m m [26] 20.25	

- c2: IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
- IF A.3/2 OR A.3/4 THEN m ELSE i - P-CSCF or S-CSCF. 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 c6: 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.
- 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 c9: option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
- 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 Pc11: 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.
- IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - adding, deleting or reading the P-Chargingc13: Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
- IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - act as subsequent entity within trust network c14: 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.

Prerequisite: A.164/2 OR A.164/3 OR A.164/4 OR A.164/5 - - 1xx

Table A.208: Supported headers within the INVITE response

ltem	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
4	Contact	[26] 20.10	m	m	[26] 20.10	i	i	
6	P-Media-Authorization	[31] 6.1	с9	c10	[31] 6.1	n/a	n/a	
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: c10:	IF A.162/26 THEN m ELSE n/		sions for me	dia authoriza	tion.			

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/6 - - 2xx

Table A.209: Supported headers within the INVITE response

Item	Header		Sending			Receiving	
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	m	m	[26] 20.1	j	j
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
2	Allow	[26] 20.5	m	m	[26] 20.5	i	i
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
8	P-Media-Authorization	[31] 6.1	с9	c10	[31] 6.1	n/a	n/a
9	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	сЗ
13	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c3:	IF A.162/14 THEN m ELSE	i the requirem	ent to be abl	e to insert its	elf in the subs	sequent tran	sactions in

a dialog.

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 (Ambiguous)

Table A.210: Supported headers within the INVITE response

Item	Header		Sending			Receiving	Receiving	
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
4	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1	
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
c1:	IF A.162/19E THEN m ELSE i -	- deleting Co	ntact header	s.				

c9: IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization.

c10: IF A.3/2 THEN m ELSE n/a - - P-CSCF.

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.211: Supported headers within the INVITE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
6	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m	
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
15	WWW-Authenticate	[26] 20.44	0		[26] 20.44	0		

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 - - 404, 413, 480, 486, 600, 603

Table A.212: Supported headers within the INVITE response

Item	Header		Sending F				Receiving	
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
8	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i	
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
12	Via	[26] 20.42	m	m	[26] 20.42	m	m	

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/18 - - 405 (Method Not Allowed)

Table A.213: Supported headers within the INVITE response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
2	Allow	[26] 20.5	m		[26] 20.5	m/o		
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
13	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/20 - - 407 (Proxy Authentication Required)

Table A.214: Supported headers within the INVITE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
6	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m	
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
11	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i	

Prerequisite: A.164/25 - - 415 (Unsupported Media Type)

Table A.215: Supported headers within the INVITE response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	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	
6	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
11	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/27 - - 420 (Bad Extension)

Table A.216: Supported headers within the INVITE response

Item	Header		Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i		
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
9	Supported	[26] 20.37	m	m	[26] 20.37	i	i		
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 that	n REGISTER							

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/28 OR A.164/41A - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.216A: Supported headers within the INVITE response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
3	Security-Server	[48] 2	c1	c1	[48] 2	n/a	n/a		
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
c1:	IF A.162/47 THEN m ELSE n/a security mechanism agreement for the session initiation protocol.								

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/34 - - 484 (Address Incomplete)

Table A.217: Supported headers within the INVITE response

Item	Header		Sending		Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
9	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite: A.164/42 - - 500 (Server Internal Error)

Table A.217A: Supported headers within the INVITE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
8	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i	
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/45 - - 503 (Service Unavailable)

Table A.217B: Supported headers within the INVITE response

Item	Header		Sending		Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
8	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Table A.218: Void

A.2.2.4.7A MESSAGE method

Prerequisite A.163/9A - - MESSAGE request

Table A.218A: Supported headers within the MESSAGE request

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	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	I	i
14	From	[26] 20.20	m	m	[26] 20.20	m	m
15	In-Reply-To	[26] 20.21	m	m	[50] 10	i	i
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	сЗ
18A	P-Access-Network-Info	[52] 4.4	c23	c23	[52] 4.4	c24	c24
18B	P-Asserted-Identity	[34] 9.1	c10	c10	[34] 9.1	c11	c11
18C	P-Called-Party-ID	[52] 4.2	c14	c14	[52] 4.2	c15	c16
18D	P-Charging-Function- Addresses	[52] 4.5	c21	c21	[52] 4.5	c22	c22
18E	P-Charging-Vector	[52] 4.6	c19	c19	[52] 4.6	c20	c20
18F	P-Preferred-Identity	[34] 9.2	X	X	[34] 9.2	c9	c9
18G	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
22	Record-Route	[26] 20.30	m	m	[26] 20.30	с7	с7
23	Reply-To	[26] 20.31	m	m	[26] 20.31	i	i
24	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
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	х	х	[48] 2.3.1	c25	c25
26	Subject	[26] 20.36	m	m	[26] 20.36	i	i
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	То	[26] 20.39	m	m	[26] 20.39	m	m
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 Å.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 THEN i ELSE n/a - the P-Called-Party-ID header extension and P-CSCF or I-CSCF.
- 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 THEN m ELSE n/a - security mechanism agreement for the session initiation protocol.
- 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.218B: Void

Prerequisite A.163/9B - - MESSAGE response

Table A.218C: Supported headers within the MESSAGE response - all remaining status-codes

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
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	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	c13	c13	[52] 4.4	c14	c14	
12B	P-Asserted-Identity	[34] 9.1	c5	c5	[34] 9.1	c6	c6	
12C	P-Charging-Function- Addresses	[52] 4.5	c11	c11	[52] 4.5	c12	c12	
12D	P-Charging-Vector	[52] 4.6	с9	n/a	[52] 4.6	c10	n/a	
12E	P-Preferred-Identity	[34] 9.2	Х	Х	[34] 9.2	c4	n/a	
12F	Privacy	[33] 4.2	с7	c7	[33] 4.2	c8	c8	
12G	Require	[26] 20.32	m	m	[26] 20.32	c15	c15	
13	Server	[26] 20.35	m	m	[26] 20.35	i	i	
14	Timestamp	[26] 20.38	i	i	[26] 20.38	i	i	
15	То	[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.

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/6 - - 2xx

Table A.218D: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
2	Authentication-Info	[26] 20.6	m	m	[26] 20.6	i	i	
4	Record-Route	[26] 20.30	m	m	[26] 20.30	с3	c3	
6	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.							

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 (Ambiguous)

Table A.218E: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving					
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status			
1	Allow	[26] 20.5	m	m	[50] 10	i	i			
2	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1			
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i			
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i			
c1:	1: IF A.162/19E THEN m ELSE i deleting Contact headers.									

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.218F: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[50] 10	i	i	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
3	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.218G: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/18 - - 405 (Method Not Allowed)

Table A.218H: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/20 - - 407 (Proxy Authentication Required)

Table A.218I: Supported headers within the MESSAGE response

Item	Header		Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[50] 10	i	i	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
3	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i	

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/25 - - 415 (Unsupported Media Type)

Table A.218J: Supported headers within the MESSAGE response

Item	Header	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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/27 - - 420 (Bad Extension)

response to a method other than REGISTER.

Table A.218K: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	m	m	[50] 10	i	i		
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i		
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								

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/28 OR A.164/41A - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.218L: Supported headers within the MESSAGE response

Item	Header	Sending				Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status			
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m			
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0			
3	Security-Server	[48] 2	c1	c1	[48] 2	n/a	n/a			
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m			
c1:	IF A.162/47 THEN m ELSE n/a security mechanism agreement for the session initiation protocol.									

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/34 - - 484 (Address Incomplete)

Table A.218M: Supported headers within the MESSAGE response

Item	Header		Sending		Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Allow	[26] 20.5	m	m	[50] 10	i	i
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Table A.218N: Void

A.2.2.4.8 NOTIFY method

Prerequisite A.163/10 - - NOTIFY request

Table A.219: Supported headers within the NOTIFY request

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	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	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6A	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	From	[26] 20.20	m	m	[26] 20.20	m	m
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	c16	c16	[52] 4.4	c17	c17
17B	P-Asserted-Identity	[34] 9.1	с8	с8	[34] 9.1	с9	с9
17C	P-Charging-Function-	[52] 4.5	c14	c14	[52] 4.5	c15	c15
	Addresses			,			,
17D	P-Charging-Vector	[52] 4.6	c12	n/a	[52] 4.6	c13	n/a
17E	P-Preferred-Identity	[34] 9.2	X	X	[34] 9.2	c3	n/a
17F	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
20	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
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	Х	Х	[48] 2.3.1	c18	c18
22B	Security-Verify	[48] 2.3.1	Х	х	[48] 2.3.1	c18	c18
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
25	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
26	То	[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

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
Co.	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 THEN m ELSE n/a security mechanism agreement for the session initiation protocol.
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

Item	Header		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-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			
10	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i			
10A	P-Access-Network-Info	[52] 4.4	c11	c11	[52] 4.4	c12	c12			
10B	P-Asserted-Identity	[34] 9.1	c3	c3	[34] 9.1	c4	c4			
10C	P-Charging-Function- Addresses	[52] 4.5	с9	с9	[52] 4.5	c10	c10			
10D	P-Charging-Vector	[52] 4.6	с7	n/a	[52] 4.6	с8	n/a			
10E	P-Preferred-Identity	[34] 9.2	Х	Х	[34] 9.2	c2	n/a			
10F	Privacy	[33] 4.2	c5	c5	[33] 4.2	c6	c6			
10G	Require	[26] 20.32	m	m	[26] 20.32	c13	c13			
10H	Server	[26] 20.35	m	m	[26] 20.35	i	i			
11	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i			
12	То	[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 i	nsertion of da	te in reques	ts and respor	ises.					
c2:	IF A.162/30A THEN m ELSE n/									
c3:	IF A.162/30 THEN m ELSE n/a within trusted networks.									
c4:	within trusted networks. 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.

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/6 AND A.164/7 - - 2xx

Table A.222: Supported headers within the NOTIFY response

		• :	
Item	Hoodor	Sandina	Pocoivina
	neager		Necelviilu

		Ref.	RFC	Profile	Ref.	RFC	Profile			
			status	status		status	status			
0A	Allow	[26] 20.5	m	m	[26] 20.5	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	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3			
5	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 routeing.									

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 (Ambiguous)

Table A.223: Supported headers within the NOTIFY response

Item	Header	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	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
c1:	IF A.162/19E THEN m ELSE i deleting Contact headers.							

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.224: Supported headers within the NOTIFY response

Item	Header	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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.225: Supported headers within the NOTIFY response

Item	Header	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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
3	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite: A.164/18 - - 405 (Method Not Allowed)

Table A.226: Supported headers within the NOTIFY response

Item	Header	Sending			Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/20 - - 407 (Proxy Authentication Required)

Table A.227: Supported headers within the NOTIFY response

Item	Header		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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m		
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i		
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i		

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/25 - - 415 (Unsupported Media Type)

Table A.228: Supported headers within the NOTIFY response

Item	Header	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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/27 - - 420 (Bad Extension)

Table A.229: Supported headers within the NOTIFY response

Item	Header	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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
5	Unsupported	[26] 20.40	m	m	[26] 20.40	с3	c3	
c3:	IF A 162/18 THEN m FLSE i reading the contents of the Unsupported header before proxying the 420							

response to a method other than REGISTER.

Prerequisite: A.164/28 OR A.164/41A - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.229A: Supported headers within the NOTIFY response

Item	Header		Sending				Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status			
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m			
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0			
3	Security-Server	[48] 2	c1	c1	[48] 2	n/a	n/a			
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m			
c1:	IF A 162/47 THEN m FLSE n/a security mechanism agreement for the session initiation protocol.									

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/34 - - 484 (Address Incomplete)

Table A.230: Supported headers within the NOTIFY response

Item	Header		Sending		Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/11 - - NOTIFY response

Prerequisite: A.164/39 - - 489 (Bad Event)

Table A.231: Supported headers within the NOTIFY response

Item	Header		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	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1		
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
c1:	IF A.4/20 THEN m ELSE i SI	P specific eve	ent notification	on 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.232: Void

A.2.2.4.9 OPTIONS method

Prerequisite A.163/12 - - OPTIONS request

Table A.233: Supported headers within the OPTIONS request

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	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	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
16	From	[26] 20.20	m	m	[26] 20.20	m	m
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	c23	c23	[52] 4.4	c24	c24
19B	P-Asserted-Identity	[34] 9.1	c10	c10	[34] 9.1	c11	c11
19C	P-Called-Party-ID	[52] 4.2	c14	c14	[52] 4.2	c15	c16
19D	P-Charging-Function- Addresses	[52] 4.5	c21	c21	[52] 4.5	c22	c22
19E	P-Charging-Vector	[52] 4.6	c19	c19	[52] 4.6	c20	c20
19F	P-Preferred-Identity	[34] 9.2	Х	Х	[34] 9.2	с9	с9
19G	P-Visited-Network-ID	[52] 4.3	c17	n/a	[52] 4.3	c18	n/a
19H	Privacy	[33] 4.2	c12	c12	[33] 4.2	c13	c13
20	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c8	с8
21	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
22	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
23	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
24	Route	[26] 20.34	m	m	[26] 20.34	m	m
24A	Security-Client	[48] 2.3.1	Х	х	[48] 2.3.1	c25	c25
24B	Security-Verify	[48] 2.3.1	х	Х	[48] 2.3.1	c25	c25
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	То	[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 Å.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 THEN i ELSE n/a - the P-Called-Party-ID header extension and P-CSCF or I-CSCF.
- 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 THEN m ELSE n/a - security mechanism agreement for the session initiation protocol.

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.234: Void

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/1 - - 100 (Trying)

Table A.235: Supported headers within the OPTIONS response

Item	Header		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			
6	То	[26] 20.39	m	m	[26] 20.39	m	m			
7	Via	[26] 20.42	m	m	[26] 20.42	m	m			
c1:	c1: IF A.162/9 THEN m ELSE i insertion of date in requests and responses.									

Table A.236: Supported headers within the OPTIONS response - all remaining status-codes

ltem	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
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	
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	c13	c13	[52] 4.4	c14	c14	
11B	P-Asserted-Identity	[34] 9.1	c5	c5	[34] 9.1	c6	c6	
11C	P-Charging-Function- Addresses	[52] 4.5	c11	c11	[52] 4.5	c12	c12	
11D	P-Charging-Vector	[52] 4.6	с9	с9	[52] 4.6	c10	c10	
11E	P-Preferred-Identity	[34] 9.2	х	х	[34] 9.2	c4	n/a	
11F	Privacy	[33] 4.2	с7	c7	[33] 4.2	с8	с8	
11G	Require	[26] 20.32	m	m	[26] 20.32	c15	c15	
11H	Server	[26] 20.35	m	m	[26] 20.35	i	i	
12	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i	
13	То	[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: c2:	IF A.162/9 THEN m ELSE i i IF A.162/19A OR A.162/19B Th					he Organiza	tion 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.

Prerequisite: A.164/6 - - 2xx

Table A.237: Supported headers within the OPTIONS response

Item	Header		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	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
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	
9	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	с3	
12	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.							

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 (Ambiguous)

Table A.238: Supported headers within the OPTIONS response

Item	Header	Sending				Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i		
3	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1		
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i		
c1:	IF A.162/19E THEN m ELSE i deleting Contact headers.								

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.239: Supported headers within the OPTIONS response

Item	Header		Sending		Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
7	Supported	[26] 20.37	m	m	[26] 20.37	i	İ
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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.240: Supported headers within the OPTIONS response

Item	Header			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite: A.164/18 - - 405 (Method Not Allowed)

Table A.241: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
2	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/20 - - 407 (Proxy Authentication Required)

Table A.242: Supported headers within the OPTIONS response

Item	Header		Sending		Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/25 - - 415 (Unsupported Media Type)

Table A.243: Supported headers within the OPTIONS response

Item	Header	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	[26] 20.5	i	i	
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/27 - - 420 (Bad Extension)

response to a method other than REGISTER.

Table A.244: Supported headers within the OPTIONS response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
7	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3	
c3:	IF A.162/18 THEN m ELSE i	reading the c	ontents of th	e Unsupporte	ed header be	fore proxying	the 420	

Prerequisite: A.164/28 OR A.164/41A - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.244A: Supported headers within the OPTIONS response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
3	Security-Server	[48] 2	c1	c1	[48] 2	n/a	n/a	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
c1:	IF A.162/47 THEN m ELSE n/a	security m	echanism ac	reement for	the session ir	nitiation prote	col.	

Prerequisite A.163/13 - - OPTIONS response

Prerequisite: A.164/34 - - 484 (Address Incomplete)

Table A.245: Supported headers within the OPTIONS response

Item	Header	Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Table A.246: Void

A.2.2.4.10 PRACK method

Prerequisite A.163/14 - - PRACK request

Table A.247: Supported headers within the PRACK request

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	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	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
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	c14	c14	[52] 4.4	c15	c15
16B	P-Charging-Function-	[52] 4.5	c12	c12	[52] 4.5	c13	c13
	Addresses						
16C	P-Charging-Vector	[52] 4.6	c10	n/a	[52] 4.6	c11	n/a
16D	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
20	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	с7
21	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
22	Route	[26] 20.34	m	m	[26] 20.34	m	m
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	То	[26] 20.39	m	m	[26] 20.39	m	m
26	User-Agent	[26] 20.41	m	m	[26] 20.41	i	İ
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 0 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.
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.248: Void

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/1 - - 100 (Trying)

Table A.249: Supported headers within the PRACK response

Item	Header		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			
6	То	[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 THEN m ELSE i insertion of date in requests and responses.									

Prerequisite A.163/15 - - PRACK response

Table A.250: Supported headers within the PRACK response - all remaining status-codes

Item	Header		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-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	с9	с9	[52] 4.4	c10	c10	
10B	P-Charging-Function- Addresses	[52] 4.5	c7	c7	[52] 4.5	c8	c8	
10C	P-Charging-Vector	[52] 4.6	c5	n/a	[52] 4.6	c6	n/a	
10D	Privacy	[33] 4.2	c3	с3	[33] 4.2	c4	c4	
10E	Require	[26] 20.32	m	m	[26] 20.32	c11	c11	
10F	Server	[26] 20.35	m	m	[26] 20.35	i	i	
11	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i	
12	То	[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		te in reques	ts and respor		•	•	
c2:	IF A.3/2 OR A.3/4 THEN m EL							
c3:	IF A.162/31 THEN m ELSE n/a	a a privacy	mechanism t	for the Session	on Initiation Pi	rotocol (SIP)	١.	
c4:	IF A.162/31D OR A.162/31G T option "header" or application of							
c5:	IF A.162/45 THEN m ELSE n/a							
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							
c8:	IF A.162/44A THEN m ELSE IF Function-Addresses header be Addresses header extension.			_		•		
-0-	IE A 400/40 THEN ELOF IE A	400/44 TUE						

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.

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/6 - - 2xx

Table A.251: Supported headers within the PRACK response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
0B	Authentication-Info	[26] 20.6	m	m	[26] 20.6	i	i	
1	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.

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 (Ambiguous)

Table A.252: Supported headers within the PRACK response

Item	Header	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	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1			
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i			
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i			
c1:										

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.253: Supported headers within the PRACK response

Item	Header		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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.254: Supported headers within the PRACK response

Item	Header	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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
3	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/18 - - 405 (Method Not Allowed)

Table A.255: Supported headers within the PRACK response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/20 - - 407 (Proxy Authentication Required)

Table A.256: Supported headers within the PRACK response

Item	Header		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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i	

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/25 - - 415 (Unsupported Media Type)

Table A.257: Supported headers within the PRACK response

Item	Header		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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/27 - - 420 (Bad Extension)

Table A.258: Supported headers within the PRACK response

Item	Header		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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i		

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/28 OR A.164/41A - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.258A: Supported headers within the PRACK response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
3	Security-Server	[48] 2	c1	c1	[48] 2	n/a	n/a		
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
c1:	IF A.162/47 THEN m ELSE n/a	security m	echanism ac	reement for	the session ir	itiation proto	col.		

Prerequisite A.163/15 - - PRACK response

Prerequisite: A.164/34 - - 484 (Address Incomplete)

Table A.259: Supported headers within the PRACK response

Item	Header	Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Table A.260: Void

A.2.2.4.11 REFER method

Prerequisite A.163/16 - - REFER request

Table A.261: Supported headers within the REFER request

Item	Header		Sending		Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	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
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	İ
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
11	From	[26] 20.20	m	m	[26] 20.20	m	m
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	c22	c22	[52] 4.4	c23	c23
14B	P-Asserted-Identity	[34] 9.1	с9	с9	[34] 9.1	c10	c10
14C	P-Called-Party-ID	[52] 4.2	c13	c13	[52] 4.2	c14	c15
14D	P-Charging-Function- Addresses	[52] 4.5	c20	c20	[52] 4.5	c21	c21
14E	P-Charging-Vector	[52] 4.6	c18	c18	[52] 4.6	c19	c19
14F	P-Preferred-Identity	[34] 9.2	Х	Х	[34] 9.2	c8	c8
14G	P-Visited-Network-ID	[52] 4.3	c16	n/a	[52] 4.3	c17	n/a
14H	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
17	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
18	Refer-To	[36] 3	c3	c3	[36] 3	c4	c4
19	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
20	Route	[26] 20.34	m	m	[26] 20.34	m	m
20A	Security-Client	[48] 2.3.1	Х	Х	[48] 2.3.1	c24	c24
20B	Security-Verify	[48] 2.3.1	х	Х	[48] 2.3.1	c24	c24
20C	Subject	[26] 20.36	m	m	[26] 20.36	i	i
21	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
22	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
23	То	[26] 20.39	m	m	[26] 20.39	m	m
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 Å.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 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.162/37 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 THEN i ELSE n/a - the P-Called-Party-ID header extension and P-CSCF or I-CSCF.
- 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 THEN m ELSE n/a - security mechanism agreement for the session initiation protocol.

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.262: Void

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/1 - - 100 (Trying)

Table A.263: Supported headers within the REFER response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	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	
6	То	[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 THEN m ELSE i i	nsertion of da	te in request	s and respor	ises.			

Table A.264: Supported headers within the REFER response - all remaining status-codes

Header	Sending			Receiving			
	Ref.	RFC	Profile	Ref.	RFC	Profile	
			status		status	status	
		m	m		m	m	
Content-Disposition		m	m	[26] 20.11	i	i	
Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i	
Content-Language	[26] 20.13	m	m	[26] 20.13	i	i	
Content-Length	[26] 20.14	m	m	[26] 20.14	m	m	
Content-Type	[26] 20.15	m	m	[26] 20.15	i	i	
Cseq	[26] 20.16	m	m	[26] 20.16	m	m	
Date	[26] 20.17	m	m	[26] 20.17	c1	c1	
From	[26] 20.20	m	m	[26] 20.20	m	m	
MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i	
Organization	[26] 20.25	m	m	[26] 20.25	c2	c2	
P-Access-Network-Info	[52] 4.4	c12	c12	[52] 4.4	c13	c13	
P-Asserted-Identity	[34] 9.1	c4	c4	[34] 9.1	c5	c5	
P-Charging-Function-	[52] 4.5	c10	c10	[52] 4.5	c11	c11	
P-Charging-Vector	[52] 4.6	c8	c8	[52] 4.6	с9	с9	
P-Preferred-Identity	[34] 9.2	Х	X	[34] 9.2	c3	n/a	
Privacy	[33] 4.2	c6	c6	[33] 4.2	c7	с7	
Require	[26] 20.32	m	m	[26] 20.32	c14	c14	
Server	[26] 20.35	m	m	[26] 20.35	i	i	
Timestamp	[26] 20.38	m	m	[26] 20.38	i	i	
То	[26] 20.39	m	m	[26] 20.39	m	m	
User-Agent	[26] 20.41	m	m	[26] 20.41	i	i	
Via	[26] 20.42	m	m	[26] 20.42	m	m	
Warning	[26] 20.43	m	m	[26] 20.43	i	i	
IF A.162/9 THEN m ELSE i	insertion of da	te in reques	ts and respor	nses.			
IF A.162/19A OR A.162/19B TI	HEN m ELSE	i reading,	adding or co	ncatenating tl	he Organiza	tion headei	
	Content-Language Content-Length Content-Type Cseq Date From MIME-Version Organization P-Access-Network-Info P-Asserted-Identity P-Charging-Function-Addresses P-Charging-Vector P-Preferred-Identity Privacy Require Server Timestamp To User-Agent Via Warning IF A.162/9 THEN m ELSE i i IF A.162/30A THEN m ELSE in	Content-Disposition [26] 20.11 Content-Encoding [26] 20.12 Content-Language [26] 20.13 Content-Length [26] 20.14 Content-Type [26] 20.15 Cseq [26] 20.16 Date [26] 20.21 From [26] 20.20 MIME-Version [26] 20.24 Organization [26] 20.25 P-Access-Network-Info [52] 4.4 P-Asserted-Identity [34] 9.1 P-Charging-Function-Addresses [52] 4.5 P-Charging-Vector [52] 4.6 P-Preferred-Identity [34] 9.2 Privacy [33] 4.2 Require [26] 20.32 Server [26] 20.35 Timestamp [26] 20.38 To [26] 20.39 User-Agent [26] 20.41 Via [26] 20.42 Warning [26] 20.43 IF A.162/9 THEN m ELSE i insertion of dall F A.162/19A OR A.162/19B THEN m ELSE IF A.162/30A THEN m ELSE IF A act as fir	Content-Disposition [26] 20.11 m Content-Encoding [26] 20.12 m Content-Language [26] 20.13 m Content-Length [26] 20.14 m Content-Type [26] 20.15 m Cseq [26] 20.16 m Date [26] 20.17 m From [26] 20.20 m MIME-Version [26] 20.24 m Organization [26] 20.25 m P-Access-Network-Info [52] 4.4 c12 P-Asserted-Identity [34] 9.1 c4 P-Charging-Function-Addresses [52] 4.5 c10 P-Preferred-Identity [34] 9.2 x P-Preferred-Identity [34] 9.2 x Privacy [33] 4.2 c6 Require [26] 20.32 m Server [26] 20.35 m Timestamp [26] 20.38 m To [26] 20.39 m User-Agent [26] 20.41 m Vi	Call-ID [26] 20.8 m m Content-Disposition [26] 20.11 m m Content-Encoding [26] 20.12 m m Content-Language [26] 20.13 m m Content-Length [26] 20.14 m m Content-Type [26] 20.15 m m Cseq [26] 20.15 m m Date [26] 20.16 m m From [26] 20.20 m m MIME-Version [26] 20.24 m m Organization [26] 20.25 m m P-Access-Network-Info [52] 4.4 c12 c12 P-Asserted-Identity [34] 9.1 c4 c4 P-Charging-Function-Addresses Addresses a c8 P-Preferred-Identity [34] 9.2 x x Privacy [33] 4.2 c6 c6 Require [26] 20.32 m m Server [26] 20.35 <t< td=""><td>Call-ID [26] 20.8 m m [26] 20.8 Content-Disposition [26] 20.11 m m [26] 20.11 Content-Encoding [26] 20.12 m m [26] 20.12 Content-Language [26] 20.13 m m [26] 20.13 Content-Length [26] 20.14 m m [26] 20.14 Content-Type [26] 20.15 m m [26] 20.15 Cseq [26] 20.15 m m [26] 20.15 Cseq [26] 20.16 m m [26] 20.15 Cseq [26] 20.17 m m [26] 20.16 Date [26] 20.20 m m [26] 20.16 Date [26] 20.20 m m [26] 20.20 MIME-Version [26] 20.20 m m [26] 20.24 Organization [26] 20.25 m m [26] 20.25 P-Access-Network-Info [52] 4.4 c12 c12 [52] 4.4 P-Asserted-Identity [34]</td><td>Call-ID [26] 20.8 m m [26] 20.8 m Content-Disposition [26] 20.11 m m [26] 20.11 i Content-Encoding [26] 20.12 m m [26] 20.12 i Content-Language [26] 20.13 m m [26] 20.13 i Content-Length [26] 20.14 m m [26] 20.14 m Content-Type [26] 20.15 m m [26] 20.15 i Cseq [26] 20.15 m m [26] 20.15 i Cseq [26] 20.15 m m [26] 20.15 i Cseq [26] 20.15 m m [26] 20.16 m Date [26] 20.17 m m [26] 20.17 c1 From [26] 20.20 m m [26] 20.20 m MIME-Version [26] 20.24 m m [26] 20.25 c2 P-Access-Network-Info [52] 4.4 c12 c12</td></t<>	Call-ID [26] 20.8 m m [26] 20.8 Content-Disposition [26] 20.11 m m [26] 20.11 Content-Encoding [26] 20.12 m m [26] 20.12 Content-Language [26] 20.13 m m [26] 20.13 Content-Length [26] 20.14 m m [26] 20.14 Content-Type [26] 20.15 m m [26] 20.15 Cseq [26] 20.15 m m [26] 20.15 Cseq [26] 20.16 m m [26] 20.15 Cseq [26] 20.17 m m [26] 20.16 Date [26] 20.20 m m [26] 20.16 Date [26] 20.20 m m [26] 20.20 MIME-Version [26] 20.20 m m [26] 20.24 Organization [26] 20.25 m m [26] 20.25 P-Access-Network-Info [52] 4.4 c12 c12 [52] 4.4 P-Asserted-Identity [34]	Call-ID [26] 20.8 m m [26] 20.8 m Content-Disposition [26] 20.11 m m [26] 20.11 i Content-Encoding [26] 20.12 m m [26] 20.12 i Content-Language [26] 20.13 m m [26] 20.13 i Content-Length [26] 20.14 m m [26] 20.14 m Content-Type [26] 20.15 m m [26] 20.15 i Cseq [26] 20.15 m m [26] 20.15 i Cseq [26] 20.15 m m [26] 20.15 i Cseq [26] 20.15 m m [26] 20.16 m Date [26] 20.17 m m [26] 20.17 c1 From [26] 20.20 m m [26] 20.20 m MIME-Version [26] 20.24 m m [26] 20.25 c2 P-Access-Network-Info [52] 4.4 c12 c12	

- 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.

Prerequisite: A.164/7 - - 202 (Accepted)

Table A.265: Supported headers within the REFER response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i		
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		
5	Record-Route	[26] 20.30	m	m	[26] 20.30	с3	с3		
8	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 routeing.								

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 OR A.164/35 - - 3xx or 485 (Ambiguous)

Table A.266: Supported headers within the REFER response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i		
2	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1		
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i		
c1:	IF A.162/19E THEN m ELSE i deleting Contact headers.								

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 - - 401 (Unauthorized)

Table A.267: Supported headers within the REFER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
4	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m	
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.268: Supported headers within the REFER response

Item	Header	Sending				Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
6	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i	
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite: A.164/18 - - 405 (Method Not Allowed)

Table A.269: Supported headers within the REFER response

Item	Header	Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
2	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/20 - - 407 (Proxy Authentication Required)

Table A.270: Supported headers within the REFER response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i		
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
4	Proxy-Authenticate	[26] 20.27	0		[26] 20.27	0			
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i		
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i		

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/25 - - 415 (Unsupported Media Type)

Table A.271: Supported headers within the REFER response

Item	Header		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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i		

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/27 - - 420 (Bad Extension)

response to a method other than REGISTER.

Table A.272: Supported headers within the REFER response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
8	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3	
c3:	IF A.162/18 THEN m ELSE i	reading the c	ontents of th	e Unsupporte	ed header be	fore proxying	the 420	

Prerequisite: A.164/28 OR A.164/41A - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.272A: Supported headers within the REFER response

Item	Header	Sending				Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
3	Security-Server	[48] 2	c1	c1	[48] 2	n/a	n/a		
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
c1:	IF A.162/47 THEN m ELSE n/a security mechanism agreement for the session initiation protocol.								

Prerequisite A.163/17 - - REFER response

Prerequisite: A.164/34 - - 484 (Address Incomplete)

Table A.273: Supported headers within the REFER response

Item	Header	Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Table A.274: Void

A.2.2.4.12 REGISTER method

Prerequisite A.163/18 - - REGISTER request

Table A.275: Supported headers within the REGISTER request

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	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, [49]	m	m	[26] 20.7, [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
17	From	[26] 20.20	m	m	[26] 20.20	m	m
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	c16	c16	[52] 4.4	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
20D	P-Visited-Network-ID	[52] 4.3	c10	c10	[52] 4.3	c11	c11
20E	Path	[35] 4.2	c6	c6	[35] 4.2	c6	c6
20F	Privacy	[33] 4.2	с8	c8	[33] 4.2	с9	с9
21	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	с7	c7
22	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
23	Require	[26] 20.32	m	m	[26] 20.32	c4	c4
24	Route	[26] 20.34	m	m	[26] 20.34	m	m
24A	Security-Client	[48] 2.3.1	Х	Х	[48] 2.3.1	c18	c18
24B	Security-Verify	[48] 2.3.1	Х	Х	[48] 2.3.1	c18	c18
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	То	[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

-4:	IS A 4/00 TUEN as ELOS : OID as a first accordance for a state of the
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 THEN m ELSE n/a security mechanism agreement for the session initiation protocol.
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.276: Void

Prerequisite: A.164/1 - - 100 (Trying)

Table A.277: Supported headers within the REGISTER response

Item	Header	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	m	m	
5	From	[26] 20.20	m	m	[26] 20.20	m	m	
6	То	[26] 20.39	m	m	[26] 20.39	m	m	
7	Via	[26] 20.42	m	m	[26] 20.42	m	m	

Table A.278: Supported headers within the REGISTER response - all remaining status-codes

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
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
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	с9	с9	[52] 4.4	c10	c10
11B	P-Charging-Function- Addresses	[52] 4.5	с7	с7	[52] 4.5	c8	c8
11C	P-Charging-Vector	[52] 4.6	c5	c5	[52] 4.6	c6	c6
11D	Privacy	[33] 4.2	c3	c3	[33] 4.2	c4	c4
11E	Require	[26] 20.32	m	m	[26] 20.32	c11	c11
11F	Server	[26] 20.35	m	m	[26] 20.35	i	i
12	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
13	То	[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: c2:	IF A.162/19A OR A.162/19B TH IF A.162/19C OR A.162/19D TH	EN m ELSE IEN m ELSE	i reading,	adding or co	ncatenating t	he Call-Info	header.
c3:	IF A.162/31 THEN m ELSE n/a						
c4:	IF A.162/31D OR A.162/31G TH option "header" or application of						
c5:	IF A.162/45 THEN m ELSE n/a						•
c6:	IF A.162/46 THEN m ELSE IF A Charging-Vector header before extension.	162/45 THE	Ň i ĔLSE n/a	a adding, c	deleting, read		
c7:	IF A.162/44 THEN m ELSE n/a	the P-Cha	rging-Functi	on-Addresses	s header exte	nsion.	
c8:	IF A.162/44A THEN m FLSE IF						-Charging

- 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.

Prerequisite: A.164/6 - - 2xx

Table A.279: Supported headers within the REGISTER response

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	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
2	Allow	[26] 20.5	m	m	[26] 20.5	i	i
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	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
8	Service-Route	[38] 5	c5	c5	[38] 5	c6	c7
9	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c2:	IF A.3/2 OR A.3/3A THEN m EL	SE n/a P-	CSCF or I-C	SCF (THIG).			
c3:	IF A.162/29 THEN m ELSE n/a	Path exter	nsion suppor	t.			
c4:	IF A.162/29 THEN i ELSE n/a -						
c5:	IF A.162/32 THEN m ELSE n/a						
c6:	IF A.162/32 THEN i ELSE n/a -						
c7:	IF A.162/32 THEN (IF A.3/2 THI				ute extension	and P-CSC	F.
c8:	IF A.162/36 THEN m ELSE n/a						
c9:	IF A.162/36 THEN i ELSE n/a -	- the P-Assoc	ciated-URI ex	ktension.			

Prerequisite A.163/19 - - REGISTER response

extension and P-CSCF or I-CSCF.

c10:

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 (Ambiguous)

IF A.162/36 AND A.3/2 THEN m ELSE IF A.162/36 AND A.3/3 THEN i ELSE n/a - - the P-Associated-URI

Table A.280: Supported headers within the REGISTER response

Item	Header	Sending			Receiving						
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status				
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i				
3	Contact	[26] 20.10	m	m	[26] 20.10	c2	c2				
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i				
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i				
c2:	IF A.162/19E THEN m ELSE i -	IF A.162/19E THEN m ELSE i deleting Contact headers.									

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.281: Supported headers within the REGISTER response

Header	Sending			Receiving			
	Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
Allow	[26] 20.5	m	m	[26] 20.5	i	i	
Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m	
Security-Server	[48] 2	Х	c1	[48] 2	n/a	n/a	
Supported	[26] 20.37	m	m	[26] 20.37	i	i	
WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i	
	Error-Info Proxy-Authenticate Security-Server Supported WWW-Authenticate	Allow [26] 20.5 Error-Info [26] 20.18 Proxy-Authenticate [26] 20.27 Security-Server [48] 2 Supported [26] 20.37 WWW-Authenticate [26] 20.44	Allow [26] 20.5 m Error-Info [26] 20.18 m Proxy-Authenticate [26] 20.27 m Security-Server [48] 2 x Supported [26] 20.37 m WWW-Authenticate [26] 20.44 m	Allow [26] 20.5 m m Error-Info [26] 20.18 m m Proxy-Authenticate [26] 20.27 m m Security-Server [48] 2 x c1 Supported [26] 20.37 m m WWW-Authenticate [26] 20.44 m m	Allow [26] 20.5 m m [26] 20.5 Error-Info [26] 20.18 m m [26] 20.18 Proxy-Authenticate [26] 20.27 m m [26] 20.27 Security-Server [48] 2 x c1 [48] 2 Supported [26] 20.37 m m [26] 20.37 WWW-Authenticate [26] 20.44 m m [26] 20.44	Allow [26] 20.5 m m [26] 20.5 i Error-Info [26] 20.18 m m [26] 20.18 i Proxy-Authenticate [26] 20.27 m m [26] 20.27 m Security-Server [48] 2 x c1 [48] 2 n/a Supported [26] 20.37 m m [26] 20.37 i	

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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.282: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
6	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i	
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/18 - - 405 (Method Not Allowed)

Table A.283: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
2	Allow	[26] 20.5	m	m	[26] 20.5	i	i
4	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/20 - - 407 (Proxy Authentication Required)

Table A.284: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
5	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m	
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
9	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i	

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/25 - - 415 (Unsupported Media Type)

Table A.285: Supported headers within the REGISTER response

Item	Header		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	[26] 20.5	i	i		
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
9	Supported	[26] 20.37	m	m	[26] 20.37	i	i		

Prerequisite: A.164/27 - - 420 (Bad Extension)

Table A.286: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
8	Unsupported	[26] 20.40	m	m	[26] 20.40	с3	c3	
c3:	IF A.162/17 THEN m ELSE.i							

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/28 OR A.164/41A - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.286A: Supported headers within the REGISTER response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
3	Security-Server	[48] 2	c1	c1	[48] 2	n/a	n/a		
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
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 - - 423 (Interval Too Brief)

Table A.287: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
3	Error-Info	[26] 20.18	0		[26] 20.18	0		
5	Min-Expires	[26] 20.23	m	m	[26] 20.23	i	i	
8	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/19 - - REGISTER response

Prerequisite: A.164/34 - - 484 (Address Incomplete)

Table A.288: Supported headers within the REGISTER response

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Table A.289: Void

A.2.2.4.13 SUBSCRIBE method

Prerequisite A.163/20 - - SUBSCRIBE request

Table A.290: Supported headers within the SUBSCRIBE request

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	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	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
6A	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
16	From	[26] 20.20	m	m	[26] 20.20	m	m
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	c22	c22	[52] 4.4	c23	c23
18C	P-Asserted-Identity	[34] 9.1	с9	с9	[34] 9.1	c10	c10
18D	P-Called-Party-ID	[52] 4.2	c13	c13	[52] 4.2	c14	c15
18E	P-Charging-Function- Addresses	[52] 4.5	c20	c20	[52] 4.5	c21	c21
18F	P-Charging-Vector	[52] 4.6	c18	c18	[52] 4.6	c19	c19
18G	P-Preferred-Identity	[34] 9.2	X	X	[34] 9.2	c8	c8
18H	P-Visited-Network-ID	[52] 4.3	c16	n/a	[52] 4.3	c17	n/a
18I	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
21	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	с7
22	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
23	Route	[26] 20.34	m	m	[26] 20.34	m	m
23A	Security-Client	[48] 2.3.1	х	х	[48] 2.3.1	c24	c24
23B	Security-Verify	[48] 2.3.1	х	X	[48] 2.3.1	c24	c24
24	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
25	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
26	То	[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

- 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 Å.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 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.162/37 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 THEN i ELSE n/a - the P-Called-Party-ID header extension and P-CSCF or I-CSCF.
- 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 THEN m ELSE n/a - security mechanism agreement for the session initiation protocol.
- 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.291: Void

Prerequisite A.163/21 - - SUBSCRIBE response

Table A.292: Supported headers within the SUBSCRIBE response - all status-codes

Item	Header		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
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	
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	c12	c12	[52] 4.4	c13	c13	
10C	P-Asserted-Identity	[34] 9.1	c4	c4	[34] 9.1	c5	c5	
10D	P-Charging-Function- Addresses	[52] 4.5	c10	c10	[52] 4.5	c11	c11	
10E	P-Charging-Vector	[52] 4.6	c8	с8	[52] 4.6	с9	с9	
10F	P-Preferred-Identity	[34] 9.2	Х	Х	[34] 9.2	c3	n/a	
10G	Privacy	[33] 4.2	c6	c6	[33] 4.2	с7	с7	
10H	Require	[26] 20.32	m	m	[26] 20.32	c14	c14	
101	Server	[26] 20.35	m	m	[26] 20.35	i	i	
11	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i	
12	То	[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.

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/6 AND A.164/7 - - 2xx

Table A.293: Supported headers within the SUBSCRIBE response

Item	Header		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	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	
3	Record-Route	[26] 20.30	m	m	[26] 20.30	с3	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 routeing.							

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 (Ambiguous)

Table A.294: Supported headers within the SUBSCRIBE response

Item	Header		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	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1		
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i		
c1:	IF A.162/19E THEN m ELSE i deleting Contact headers.								

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.295: Supported headers within the SUBSCRIBE response

Item	Header		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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
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.164/50 OR A.164/51 - - 404, 413, 480, 486, 500, 600, 603

Table A.296: Supported headers within the SUBSCRIBE response

Item	Header		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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
3	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i	
5	Supported	[26] 20 37	m	m	[26] 20 37	i	i	

Prerequisite: A.164/18 - - 405 (Method Not Allowed)

Table A.297: Supported headers within the SUBSCRIBE response

Item	Header		Sending		Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/20 - - 407 (Proxy Authentication Required)

Table A.298: Supported headers within the SUBSCRIBE response

Item	Header		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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
2	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/25 - - 415 (Unsupported Media Type)

Table A.299: Supported headers within the SUBSCRIBE response

Item	Header	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	[26] 20.5	i	i	
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/27 - - 420 (Bad Extension)

Table A.300: Supported headers within the SUBSCRIBE response

Item	Header	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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
5	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3	
c3:	IF A.162/18 THEN m ELSE i	reading the c	ontents of th	e Unsupport	ed header be	fore proxying	the 420	

response to a method other than REGISTER.

Prerequisite: A.164/28 OR A.164/41A - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.300A: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m	
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0	
3	Security-Server	[48] 2	c1	c1	[48] 2	n/a	n/a	
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m	
c1:	IF A.162/47 THEN m ELSE n/a	security m	echanism ac	reement for	the session ir	nitiation prote	col.	

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/29 - - 423 (Interval Too Brief)

Table A.301: Supported headers within the SUBSCRIBE response

Item	Header	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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
2	Min-Expires	[26] 20.23	m	m	[26] 20.23	i	i	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	İ	

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/34 - - 484 (Address Incomplete)

Table A.302: Supported headers within the SUBSCRIBE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
			อเลเนอ	วเลเนอ		อเลเนอ	่อเลเนอ
0A	Allow	[26] 20.5	m	m	[26] 20.5	i	i
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/21 - - SUBSCRIBE response

Prerequisite: A.164/39 - - 489 (Bad Event)

Table A.303: Supported headers within the SUBSCRIBE response

Item	Header	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	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
c1:	IF A.4/20 THEN m ELSE i SIP specific event notification extension.						
NOTE:	c1 refers to the LIA rele major of	anahility ac th	ic ic the cac	of a provide	hat also asts	ac a LIA cno	cifically for

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.164/45 - - 503 (Service Unavailable)

Table A.303A: Supported headers within the SUBSCRIBE response

Item	Header	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	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
3	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i	
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Table A.304: Void

A.2.2.4.14 UPDATE method

Prerequisite A.163/22 - - UPDATE request

Table A.305: Supported headers within the UPDATE request

Item	Header		Sending			Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	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	[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	с8	
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	
17	From	[26] 20.20	m	m	[26] 20.20	m	m	
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	
20	Organization	[26] 20.25	m	m	[26] 20.25	c3	c3	
20A	P-Access-Network-Info	[52] 4.4	c16	c16	[52] 4.4	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	
20D	Privacy	[33] 4.2	c10	c10	[33] 4.2	c11	c11	
21	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	с9	с9	
22	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m	
23	Record-Route	[26] 20.30	m	m	[26] 20.30	с7	c7	
24	Require	[26] 20.32	m	m	[26] 20.32	c5	c5	
25A	Security-Client	[48] 2.3.1	х	Х	[48] 2.3.1	c18	c18	
25B	Security-Verify	[48] 2.3.1	х	Х	[48] 2.3.1	c18	c18	
25	Route	[26] 20.34	m	m	[26] 20.34	m	m	
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	То	[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	

SUBSCRIBE and NOTIFY.

c18: NOTE:

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

IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol. c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for

Table A.306: Void

Prerequisite A.163/22 - - UPDATE response

Table A.307: Supported headers within the UPDATE response - all remaining status-codes

Item	Header		Sending			Receiving	
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
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	сЗ
3	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	с3
4	Content-Language	[26] 20.13	m	m	[26] 20.13	i	с3
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
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	c11	c11	[52] 4.4	c12	c12
10C	P-Charging-Function- Addresses	[52] 4.5	с9	c9	[52] 4.5	c10	c10
10D	P-Charging-Vector	[52] 4.6	с7	n/a	[52] 4.6	с8	n/a
10E	Privacy	[33] 4.2	c5	c5	[33] 4.2	c6	c6
10F	Require	[26] 20.32	m	m	[26] 20.32	c13	c13
10G	Server	[26] 20.35	m	m	[26] 20.35	i	i
11	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
12	То	[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 ir						
c2:	IF A.162/19A OR A.162/19B TH				ncatenating tl	ne Organiza [.]	tion heade
c3:	IF A.3/2 OR A.3/4 THEN m ELS						
c4:	IF A.162/19C OR A.162/19D TH						
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.						
с7:	IF A.162/45 THEN m ELSE n/a						
c8:	IF A.162/46 THEN m ELSE IF A Charging-Vector header before						

- c9: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
- IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - adding, deleting or reading the P-Chargingc10: 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
- IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - act as subsequent entity within trust network c12: for access network information that can route outside the trust network, the P-Access-Network-Info header
- 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.

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/6 - - 2xx

Table A.308: Supported headers within the UPDATE response

Item	Header	Sendina	Receiving

		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	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
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
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
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c3:	IF A.162/15 THEN o ELSE i - and downstream direction who			e to use sepa	rate URIs in t	he upstream	direction

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 - - 3xx

Table A.309: Supported headers within the UPDATE response

Item	Header		Sending		Receiving					
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status			
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i			
2	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1			
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i			
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i			
c1:										

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.309A: Supported headers within the UPDATE response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i		
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
3	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m		
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i		
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 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.310: Supported headers within the UPDATE response

Item	Header		Sending			Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile		
			status	status		status	status		
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i		
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
5	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i		
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i		

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/18 - - 405 (Method Not Allowed)

Table A.311: Supported headers within the UPDATE response

Item	Header	Sending			Receiving		
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/20 - - 407 (Proxy Authentication Required)

Table A.312: Supported headers within the UPDATE response

Item	Header		Sending			Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i		
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
4	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m		
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i		
8	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i		

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/25 - - 415 (Unsupported Media Type)

Table A.313: Supported headers within the UPDATE response

Item	Header	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	[26] 20.5	i	i	
6	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
10	Supported	[26] 20.37	m	m	[26] 20.37	i	i	

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/27 - - 420 (Bad Extension)

Table A.314: Supported headers within the UPDATE response

Item	Header		Sending		Receiving			
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status	
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i	
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i	
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i	
7	Unsupported	[26] 20.40	m	m	[26] 20.40	с3	c3	
c3:	IF A.162/18 THEN m FLSE i	reading the c	contents of th	e Unsupport	ed header be	fore proxying	the 420	

response to a method other than REGISTER.

Prerequisite A.163/23 - - UPDATE response

Prerequisite: A.164/28 OR A.164/41A - - 421 (Extension Required), 494 (Security Agreement Required)

Table A.314A: Supported headers within the UPDATE response

Item	Header		Sending		Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	0	0	[26] 20.5	m	m		
2	Error-Info	[26] 20.18	0	0	[26] 20.18	0	0		
3	Security-Server	[48] 2	c1	c1	[48] 2	n/a	n/a		
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m		
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.164/35 - - 485 (Ambiguous)

Table A.315: Supported headers within the UPDATE response

Item	Header		Sending		Receiving				
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status		
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i		
2	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1		
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i		
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i		
c1:	IF A.162/19E THEN m ELSE i deleting Contact headers.								

Table A.316: Void

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 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
	Capabilities within main protocol			
	Extensions			
22	Integration of resource management and SIP?	[30]	0	m
23	Grouping of media lines	[53]	0	c1
24	Mapping of Media Streams to Resource Reservation Flows	[54]	0	c1
25	SDP Bandwidth Modifiers for RTCP Bandwidth	[56]	0	o (NOTE 1)

c1: IF A.3/1 THEN m ELSE n/a - - UE role.

NOTE 1: For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified.

A.3.2.2 SDP types

Table A.318: SDP types

Item	Туре		Sending		Receiving			
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
	Session level description							
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	0		[39] 5.4			
5	u= (URI of description)	[39] 5.5	0	n/a	[39] 5.5		n/a	
6	e= (email address)	[39] 5.6	0	n/a	[39] 5.6		n/a	
7	p= (phone number)	[39] 5.6	0	n/a	[39] 5.6		n/a	
8	c= (connection information)	[39] 5.7	0		[39] 5.7			
9	b= (bandwidth information)	[39] 5.8	0	o (NOTE 1)	[39] 5.8			
	Time description (one or more	per descri	ption)		•	•	•	
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	0	n/a	[39] 5.10		n/a	
	Session level description (cor	ntinued)						
12	z= (time zone adjustments)	[39] 5.11	0	n/a	[39] 5.11		n/a	
13	k= (encryption key)	[39] 5.12	Х	Х	[39] 5.12	n/a	n/a	
14	a= (zero or more session attribute lines)	[39] 5.13	0		[39] 5.13			
	Media description (zero or mo	re per desc	ription)					
15	m= (media name and transport address)	[39] 5.14	0	0	[39] 5.14	m	m	
16	i= (media title)	[39] 5.4	0		[39] 5.4			
17	c= (connection information)	[39] 5.7	c1	c1	[39] 5.7			
18	b= (bandwidth information)	[39] 5.8	0	o (NOTE 1)	[39] 5.8			
19	k= (encryption key)	[39] 5.12	х	X	[39] 5.12	n/a	n/a	
20	a= (zero or more media attribute lines)	[39] 5.13	0		[39] 5.13			

c1: IF A.318/15 THEN m ELSE n/a.

NOTE 1: For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified.

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			[39] 6				
2	keywords (a=keywds)	[39] 6			[39] 6				
3	name and version of tool (a=tool)	[39] 6			[39] 6				
4	packet time (a=ptime)	[39] 6			[39] 6				
5	maximum packet time (a=maxptime)	[39] 6			[39] 6				
6	receive-only mode (a=recvonly)	[39] 6			[39] 6				
7	send and receive mode (a=sendrecv)	[39] 6			[39] 6				
8	send-only mode (a=sendonly)	[39] 6			[39] 6				
9	whiteboard orientation (a=orient)	[39] 6			[39] 6				
10	conference type (a=type)	[39] 6			[39] 6				
11	character set (a=charset)	[39] 6			[39] 6				
12	language tag (a=sdplang)	[39] 6			[39] 6				
13	language tag (a=lang)	[39] 6			[39] 6				
14	frame rate (a=framerate)	[39] 6			[39] 6				
15	quality (a=quality)	[39] 6			[39] 6				
16	format specific parameters (a=fmtp)	[39] 6			[39] 6				
17	rtpmap attribute (a=rtpmap)	[39] 6			[39] 6				
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	с3	[53] 3	c4	c4		
22	group attribute (a=group)	[53] 4	c5	c5	[53] 3	c6	c6		
c1:	IF A.317/22 THEN o ELSE n/a.		•	•		•	•		
c2:	IF A.317/22 THEN m ELSE n/a.								
c3:	IF A.317/23 THEN o ELSE n/a.								
c4:	IF A.317/23 THEN m ELSE n/a.								
c5:	IF A.317/24 THEN o ELSE n/a.								
c6:	IF A.317/24 THEN m ELSE n/a.								

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
	Capabilities within main protocol			
	Extensions			
1	Integration of resource management and SIP?	[30]	0	n/a
2	Grouping of media lines	[53]	0	c1
3	Mapping of Media Streams to Resource Reservation Flows	[54]	0	c1
4	SDP Bandwidth Modifiers for RTCP Bandwidth	[56]	0	c1
c1:	IF A.3/2 THEN m ELSE n/a P-CSCF role.			

A.3.3.2 SDP types

Table A.329: SDP types

Item	Type		Sending				
		Ref.	RFC	Profile	Ref.	RFC	Profile
			status	status		status	status
	Session level description						
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
	Time description (one or more	per descri	ption)				
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
	Session level description (cor	ntinued)					
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
	Media description (zero or mo	re per desc	ription)	•	•	•	•
15	m= (media name and transport address)	[39] 5.14	m	m	[39] 5.14	m	m
16	i= (media title)	[39] 5.4	0		[39] 5.4		
17	c= (connection information)	[39] 5.7	0		[39] 5.7		
18	b= (bandwidth information)	[39] 5.8	0		[39] 5.8		
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	0		[39] 5.13		

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	FC Profile	
		Ref.	RFC	Profile	Ref.	RFC	Profile	
			status	status		status	status	
1	category (a=cat)	[39] 6			[39] 6			
2	keywords (a=keywds)	[39] 6			[39] 6			
3	name and version of tool (a=tool)	[39] 6			[39] 6			
4	packet time (a=ptime)	[39] 6			[39] 6			
5	maximum packet time (a=maxptime)	[39] 6			[39] 6			
6	receive-only mode (a=recvonly)	[39] 6			[39] 6			
7	send and receive mode (a=sendrecv)	[39] 6			[39] 6			
8	send-only mode (a=sendonly)	[39] 6			[39] 6			
9	whiteboard orientation (a=orient)	[39] 6			[39] 6			
10	conference type (a=type)	[39] 6			[39] 6			
11	character set (a=charset)	[39] 6			[39] 6			
12	language tag (a=sdplang)	[39] 6			[39] 6			
13	language tag (a=lang)	[39] 6			[39] 6			
14	frame rate (a=framerate)	[39] 6			[39] 6			
15	quality (a=quality)	[39] 6			[39] 6			
16	format specific parameters (a=fmtp)	[39] 6			[39] 6			
17	rtpmap attribute (a=rtpmap)	[39] 6			[39] 6			
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	c3	сЗ	[53] 3	c4	c4	
22	group attribute (a=group)	[53] 4	c5	c6	[53] 3	c5	c6	
c2:	IF A.328/1 THEN m ELSE i.							
c3:	IF A.328/2 THEN o ELSE n/a.							
c4:	IF A.328/2 THEN m ELSE n/a.							
c5:	IF A.328/3 THEN o ELSE n/a.							
c6:	IF A.328/3 THEN m ELSE n/a.							

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 (informative): Change history

		1-00	-		Change history	1	1	luia :
Date	TSG #	TSG Doc.	CR Re	V	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 0.0.2 Editor's internal draft Version 0.0.3 Submitted to CN1 SIP adhoc	1		
					#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			
		N1-010092			template and styles Version 0.0.7 Reflecting updates of some			
4.4/00/04		N4 040000			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			

D-1	T00 "	TOC 5	00	1-	Change history			lwo :
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
					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			
10/01/02		141 020103			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			
01/02/02		N1-020459		1	Version 1.2.0 incorporating results of CN1		1	
					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.			
					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).			
					In addition N1-020409, agreed at CN1#22			
					but missed from the previous version, was			
					also implemented.			
					References have been resequenced.			
02/03/02					Editorial clean-up by ETSI/MCC.	2.0.0	2.0.1	
11/03/02		NP-			The draft was approved, and 3GPP TS	2.0.1	5.0.0	
	CN#15	020049			24.229 was then to be issued in Rel-5 under			
0000 55	NID 45	ND	001	ļ.	formal change control.	F C C	F 4 0	N14
2002-06	NP-16	NP-	004	1	S-CSCF Actions on Authentication Failure	5.0.0	5.1.0	N1-
0000 55	ND 45	020230	007	_	 	F C C	F 4 2	020903
2002-06	NP-16	NP-	005	2	Disallow Parallel Registrations	5.0.0	5.1.0	N1-
0000	NIE :	020230	0.0-	<u> </u>	Luc e			020959
2002-06	NP-16	NP-	007	1	Hiding	5.0.0	5.1.0	N1-
0000 00	NID 40	020230	000		Owner the series of the series	F 0 0	540	020910
2002-06	NP-16	NP-	800	8	Support for services for unregistered users	5.0.0	5.1.0	
		020312	<u> </u>			<u> </u>	1	<u> </u>

D-1-	T00 #	TOO Date	lon	In	Change history	101.1	IN1	WO data
Date	TSG #	TSG Doc.	CR 009	Rev	Subject/Comment	Old	New	WG doc
2002-06			009	1	Not implemented nor implementable. In the meeting report CN1#24 under doc N1-			N1- 020921
					021513 it is shown that CR095r2 supercedes			020921
					009r1 if 095r2 was to be approved in CN#16			
					(but unfortunately 009r1 was also approved			
					in the the CN#16 draft minutes).			
2002-06	NP-16	NP-	019		MGCF procedure clarification	5.0.0	5.1.0	N1-
2002 00		020231	0.0		In Co. procedure clarinoalier	0.0.0	00	020788
2002-06	NP-16	NP-	020	2	MGCF procedure error cases	5.0.0	5.1.0	N1-
2002 00	141 10	020231	020	_	Nicor procedure error edece	0.0.0	0.1.0	020960
2002-06	NP-16	NP-	022	1	Abbreviations clean up	5.0.0	5.1.0	N1-
2002 00		020231	022	1	7 to 5 to 4 to 4 to 5 to 5 to 5 to 5 to 5	0.0.0	00	020949
2002-06	NP-16	NP-	023		Clarification of SIP usage outside IM CN	5.0.0	5.1.0	N1-
2002 00		020231	020		subsystem	0.0.0	00	020792
2002-06	NP-16	NP-	024	3	Replacement of COMET by UPDATE	5.0.0	5.1.0	
		020314						
2002-06	NP-16	NP-	025	3	Incorporation of current RFC numbers	5.0.0	5.1.0	N1-
		020231						021091
2002-06	NP-16	NP-	026	1	Clarification of B2BUA usage in roles	5.0.0	5.1.0	N1-
		020231						020941
2002-06	NP-16	NP-	028	4	Determination of MO / MT requests in I-	5.0.0	5.1.0	N1-
		020231		-	CSCF(THIG)			021248
2002-06	NP-16	NP-	030	2	P-CSCF release of an existing session	5.0.0	5.1.0	N1-
		020231			l com to the same of the same			021006
2002-06	NP-16	NP-	031	1	S-CSCF release of an existing session	5.0.0	5.1.0	N1-
		020232			a control of the cont			020939
2002-06	NP-16	NP-	033	3	SDP procedure at the UE	5.0.0	5.1.0	N1-
		020232						020971
2002-06	NP-16	NP-	035	1	AS Procedures corrections	5.0.0	5.1.0	N1-
		020232						020934
2002-06	NP-16	NP-	036	8	Corrections to SIP Compression	5.0.0	5.1.0	N1-
		020232			·			021499
2002-06	NP-16	NP-	037	1	Enhancement of S-CSCF and I-CSCF	5.0.0	5.1.0	N1-
		020232			Routing Procedures for interworking with			020928
					external networks			
2002-06	NP-16	NP-	041	2	Delivery of IMS security parameters from S-	5.0.0	5.1.0	N1-
		020232			CSCF to the P-CSCF by using proprietary			021003
					auth-param			
2002-06	NP-16	NP-	045		Cleanup of request / response terminology -	5.0.0	5.1.0	N1-
		020232			clause 5			020835
2002-06	NP-16	NP-	046		Cleanup of request / response terminology -	5.0.0	5.1.0	N1-
		020232			clause 6			020836
2002-06	NP-16	NP-	047	2	Simplification of profile tables	5.0.0	5.1.0	N1-
		020232						021059
2002-06	NP-16	NP-	049		Forking options	5.0.0	5.1.0	N1-
0000 00	ND 15	020232	0.55	<u> </u>				020839
2002-06	NP-16	NP-	050	1	Media-Authorization header corrections	5.0.0	5.1.0	
0000 55	ND 45	020315	0.5 :	 	01 5.4 19 11 (0.0000)	5 0 0	F 1 5	NI.
2002-06	NP-16	NP-	051	1	Clause 5.4 editorials (S-CSCF)	5.0.0	5.1.0	N1-
0000 55	ND 45	020233	0.50	-		5 0 0	F 1 5	020950
2002-06	NP-16	NP-	053	2	Integrity protection signalling from the P-	5.0.0	5.1.0	N1-
	ND 46	020233	05.1	-	CSCF to the S-CSCF	F 0 0	F 4 ^	021007
0000.00		NP-	054		Representing IM CN subsystem functional	5.0.0	5.1.0	N1-
2002-06	NP-16		1	-	entities in profile table roles Clause 4 editorials	5.0.0	5.1.0	020847
		020233	055		ICIAUSE 4 EDITORAIS	ເວ.ປ.ປ	15.1.0	N1-
2002-06		NP-	055		Claddo i Gallorialo	0.0.0	01110	
2002-06	NP-16	NP- 020233						020848
	NP-16	NP- 020233 NP-	055 056		Clause 5.8 editorials (MRFC)	5.0.0	5.1.0	020848 N1-
2002-06	NP-16 NP-16	NP- 020233 NP- 020233	056	4	Clause 5.8 editorials (MRFC)	5.0.0	5.1.0	020848 N1- 020849
2002-06	NP-16 NP-16	NP- 020233 NP- 020233 NP-		1	Clause 5.8 editorials (MRFC) Annex A editorials, including precondition			020848 N1- 020849 N1-
2002-06 2002-06 2002-06	NP-16 NP-16 NP-16	NP- 020233 NP- 020233 NP- 020233	056 057		Clause 5.8 editorials (MRFC) Annex A editorials, including precondition additions	5.0.0	5.1.0	020848 N1- 020849 N1- 021001
2002-06	NP-16 NP-16 NP-16	NP- 020233 NP- 020233 NP- 020233 NP-	056	1 2	Clause 5.8 editorials (MRFC) Annex A editorials, including precondition	5.0.0	5.1.0	020848 N1- 020849 N1- 021001 N1-
2002-06 2002-06 2002-06	NP-16 NP-16 NP-16 NP-16	NP- 020233 NP- 020233 NP- 020233	056 057		Clause 5.8 editorials (MRFC) Annex A editorials, including precondition additions	5.0.0	5.1.0	020848 N1- 020849 N1- 021001

	TSG #	15/2 1300			0-1	01.	NI NI	WC :
∠002-06	NID 40	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
	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-	064		Incorporation of previously agreed	5.0.0	5.1.0	N1-
2002-06	NP-16	020234 NP-	065		corrections to clause 5.2.5.2 (N1-020416) Clause 7.2 editorial corrections	5.0.0	5.1.0	021004 N1-
2002-06	NP-16	020234 NP-	067	2	S-CSCF routing of MO calls	5.0.0	5.1.0	021005 N1-
2002-06	NP-16	020234 NP-	068	1	I-CSCF routeing of dialog requests	5.0.0	5.1.0	021097 N1-
	NP-16	020234 NP-	069	2	Definition of the Tokanised-by parameter	5.0.0	5.1.0	021078 N1-
		020234			,			021096
	NP-16	NP- 020235	070	3	SDP procedures at UE	5.0.0	5.1.0	N1- 021453
	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 implicitely 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-	081	2		5.0.0	5.1.0	N1-
2002-06	NP-16	020235 NP-	082	1	Interrogation at I-CSCF in 24.229 Introduction of Visited_Network_ID p-header	5.0.0	5.1.0	021469 N1-
2002-06	NP-16	020235 NP-	084	1	MRFC register addresses	5.0.0	5.1.0	021433 N1-
2002-06	NP-16	020236 NP-	085	1	MRFC INVITE interface editor's notes	5.0.0	5.1.0	021434 N1-
2002-06	NP-16	020236 NP-	086	1	MRFC OPTIONS interface editor's notes	5.0.0	5.1.0	021470 N1-
2002-06	NP-16	020236 NP-	087		MRFC PRACK & INFO editor's notes	5.0.0	5.1.0	021471 N1-
2002-06	NP-16	020236 NP-	088	1	MGCF OPTIONS interface editor's notes	5.0.0	5.1.0	021159 N1-
2002-06	NP-16	020236 NP-	089	1	MGCF reINVITE editor's notes	5.0.0	5.1.0	021472 N1-
2002-06	NP-16	020236 NP-	090	1	3PCC AS editor's notes	5.0.0	5.1.0	021161 N1-
		020237 NP-	091		AS acting as terminating UA editor's notes	5.0.0	5.1.0	021162 N1-
	NP-16	020237 NP-		1	AS acting as originating UA editor's notes	5.0.0	5.1.0	021163 N1-
		020237	092	1				021466
	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-	097	1	SDP types	5.0.0	5.1.0	N1-
2002-06	NP-16	020237 NP- 020237	100	1	Removal of State from profile tables	5.0.0	5.1.0	021467 N1- 021173

Deta	TCO "	TCC D	CD	D	Change history	01-1	New	WC da
Date 2002-06	TSG #	TSG Doc.	CR 101	Rev	Subject/Comment	Old 5.0.0	New 5.1.0	WG doc
		020238			Editor's note cleanup - clause 3			N1- 021174
2002-06		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-	106		Editor's note cleanup - clause 5.4 and	5.0.0	5.1.0	N1-
2002-06	NP-16	020238 NP-	107		deletion of void subclauses Editor's note cleanup - clause 5.5 and	5.0.0	5.1.0	021179 N1-
2002-06	NP-16	020238 NP-	110		deletion of void subclauses Editor's note cleanup - clause 6	5.0.0	5.1.0	021180 N1-
2002-06	NP-16	020238 NP-	111	-	Editor's note cleanup - clause 9	5.0.0	5.1.0	021183 N1-
2002-06		020238 NP-	113	1	SIP Default Timers	5.0.0	5.1.0	021184 N1-
		020239						021465
2002-06		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-	129	1	Introduction of P-Access-Network-Info	5.0.0	5.1.0	N1-
2002-06	NP-16	020240 NP-	130	2	header Usage of Path and P-Service Route	5.0.0	5.1.0	021498 N1-
2002-06	NP-16	020240 NP-	133		Removal of Referred-By header from	5.0.0	5.1.0	021508 N1-
2002-06	NP-16	020240 NP-	134		specification Handling of Record-Route header in profile	5.0.0	5.1.0	021354 N1-
2002-06	NP-16	020240 NP-	135	1	tables Asserted identities and privacy	5.0.0	5.1.0	021357
2002-06	NP-16	020312 NP-	136	-	Removal of caller preferences from	5.0.0	5.1.0	N1-
2002-06		020240 NP-	137		specification Substitution of REFER references	5.0.0	5.1.0	021359 N1-
		020240						021360
2002-06		NP- 020240	138	_	Removal of session timer from specification	5.0.0	5.1.0	N1- 021361
2002-09		NP- 020489	141	2	Adding MESSAGE to 24.229	5.1.0	5.2.0	
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-	146	2	Service profiles and implicitly registered	5.1.0	5.2.0	021303
2002-09	NP-17	020488 NP-	147		public user identities S-CSCF decides when to include IOI	5.1.0	5.2.0	N1-
2002-09	NP-17	020376 NP-	148	\vdash	Clean up XML in clause 7.6	5.1.0	5.2.0	021571 N1-
2002-09	NP-17	020376 NP-	149	-	Fix clause 5.2.7.4 header	5.1.0	5.2.0	021572 N1-
		020376						021573

					Change history			
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
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 decribe 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
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

					Change history			
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2002-12		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-	208	1	Handling of INVITE requests that do not	5.2.0	5.3.0	N1-
2002-12	NP-18	020559 NP-	209	2	contain SDP UE Registration	5.2.0	5.3.0	022098 N1-
2002-12	NP-18	020559 NP-	211	1	Usage of private user identity during	5.2.0	5.3.0	022471 N1-
2002-12	NP-18	020559 NP-	212	1	P-CSCF subscription to the users	5.2.0	5.3.0	022083 N1-
2002-12	NP-18	020559 NP-	213	2	registration-state event Handling of MT call by the P-CSCF	5.2.0	5.3.0	022084 N1-
2002-12	NP-18	020559 NP-	215		P-CSCF acting as a UA	5.2.0	5.3.0	022154 N1-
2002-12		020559 NP-	216	1	S-CSCF handling of protected registrations	5.2.0	5.3.0	021939 N1-
		020559						022085
2002-12		NP- 020560	217	1	S-CSCF handling of subscription to the users registration-state event		5.3.0	N1- 022086
2002-12		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 signaling	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-	232	1	Expires information in REGISTER response	5.2.0	5.3.0	N1-
2002-12	NP-18	020560 NP-	235	2	Indication of successful establishment of	5.2.0	5.3.0	022095 N1-
2002-12	NP-18	020560 NP-	237		Dedicated Signalling PDP context to the UE P-CSCF sending 100 (Trying) Response for	5.2.0	5.3.0	022129 N1-
2002-12	NP-18	020560 NP-	239	1	reINVITE Correction on P-Asserted-Id, P-Preferred-Id,	5.2.0	5.3.0	021998 N1-
2002-12	NP-18	020561 NP-	240	1	Remote-Party-ID Clarifications to subclause 9.2.5	5.2.0	5.3.0	022100 N1-
2002-12		020561 NP-	242		ENUM translation	5.2.0	5.3.0	022137 N1-
		020561		1				022020
2002-12		NP- 020561	243	1	AS routing	5.2.0	5.3.0	N1- 022107
2002-12		NP- 020561	245	1	Warning header	5.2.0	5.3.0	N1- 022108
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-	249	3	MESSAGE corrections part 1	5.2.0	5.3.0	N1-
2002-12	NP-18	020561 NP-	250	2	MESSAGE corrections part 2	5.2.0	5.3.0	022455 N1-
2002-12	NP-18	020561 NP-	251	2	Security association clarifications	5.2.0	5.3.0	022456 N1-
	<u> </u>	020562		<u> </u>				022440

					Change history			
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2002-12		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	5.2.0	5.3.0	N1- 022493
2002-12	NP-18	NP-	267	1	deregistration Correction to network initiated re-	5.2.0	5.3.0	N1-
2002-12	NP-18	020563 NP-	268	1	authentication procedure Registration Expires Timer Default Setting	5.2.0	5.3.0	022449 N1-
2002-12	NP-18	020563 NP-	269	1	Clarification on Sh interface for charging	5.2.0	5.3.0	022439 N1-
2002-12	NP-18	020563 NP-	270	2	Clarifications on the scope	5.2.0	5.3.0	022465 N1-
2002-12	NP-18	020563 NP-	273	1	Add charging info for SUBSCRIBE	5.2.0	5.3.0	022500 N1-
2002-12	NP-18	020563 NP-	274	1	Profile revisions for RFC 3261 headers	5.2.0	5.3.0	022467 N1-
2002-12	NP-18	020563 NP-	275		Consistency changes for SDP procedures at	5.2.0	5.3.0	022413 N1-
2002-12	NP-18	020563 NP-	276		MGCF Proxy support of PRACK	5.2.0	5.3.0	022345 N1-
2002-12	NP-18	020563 NP-	277		Clarification of transparent handling of	5.2.0	5.3.0	022350 N1-
2002-12	NP-18	020563 NP- 020564	279	1	parameters in profile Meaning of refresh request	5.2.0	5.3.0	022351 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-	283	2	Support of comp=sigcomp parameter	5.2.0	5.3.0	022370
2002-12	NP-18	020634 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
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-	297	2	Reference corrections	5.3.0	5.4.0	N1-

					Change history			_
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
2003-03	NP-19	030049 NP-	300	1	488 message with a subset of allowed media	5.3.0	5.4.0	030301 N1-
2003-03	INF-19	030050	300	'	parameters	5.5.0	3.4.0	030245
2003-03	NP-19	NP-	301	1	Handling of Emergency Numbers in P-CSCF	5.3.0	5.4.0	N1-
		030050						030239
2003-03	NP-19	NP-	302	2	Correction of the registration state event	5.3.0	5.4.0	N1- 030268
2003-03	NIP-10	030050 NP-	305	2	package User initiated de-registration at P-CSCF	5.3.0	5.4.0	N1-
2003-03	141 -13	030050	303		User initiated de-registration at 1 -0001	3.3.0	3.4.0	030295
2003-03	NP-19	NP-	306	2	Network-initiated deregistration at UE, P-	5.3.0	5.4.0	N1-
		030050			CSCF, and S-CSCF			030296
2003-03	NP-19	NP-	307	2	UE deregistration during established dialogs	5.3.0	5.4.0	N1- 030297
2003-03	NP-19	030050 NP-	308	2	S-CSCF handling of deregistration during	5.3.0	5.4.0	N1-
2000 00	10	030050		_	established dialogs	0.0.0	0.1.0	030298
2003-03	NP-19	NP-	309	1	S-CSCF handling of established dialogs	5.3.0	5.4.0	N1-
0000.00	ND 40	030050	0.10		upon deregistration	500	5.40	030233
2003-03	INP-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-	311	1	P-CSCF handling of established dialogs	5.3.0	5.4.0	N1-
		030051			upon registration-lifetime expiration			030235
2003-03	NP-19	NP-	312	1	Correction of Authentication procedure	5.3.0	5.4.0	N1-
2002.02	ND 40	030051 NP-	242		Mixed Path header and Service-Route	F 2 0	<i>5</i> 4 0	030240
2003-03	INP-19	030051	313		operation	5.3.0	5.4.0	N1- 030127
2003-03	NP-19	NP-	315	2	Clarifications on updating the authorization	5.3.0	5.4.0	N1-
		030051			token			030255
2003-03	NP-19	NP-	318	2	Consideration of P-CSCF/PDF	5.3.0	5.4.0	N1-
2003-03	ND 10	030051 NP-	319	2	Clarification on GPRS charging information	5.3.0	5.4.0	030307 N1-
2003-03	141 - 13	030051	319		Claimcation on of No charging information	3.3.0	3.4.0	030308
2003-03	NP-19	NP-	323	1	P-Access-Network-Info procedure	5.3.0	5.4.0	N1-
		030051			corrections for the UE			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-	326	1	Updating user agent related profile tables	5.3.0	5.4.0	N1-
2000 00		030051	020		opaamig door agont rolated promo tables	0.0.0	0.1.0	030260
2003-03	NP-19	NP-	327	2	Cleanup and clarification to the registration	5.3.0	5.4.0	N1-
2003-03	ND 10	030052 NP-	328	4	and authentication procedure	5.3.0	5.4.0	030282 N1-
2003-03	INP-19	030052	320	1	Corrections to the reg event package	5.3.0	5.4.0	030230
2003-03	NP-19	NP-	330	2	Clarifications for setting up separate PDP	5.3.0	5.4.0	N1-
		030052			contexts in case of SBLP			030288
2003-03	NP-19	NP-	331	2	Handling of the P-Media-Autohorization header	5.3.0	5.4.0	N1-
2003-03	NP-19	030052 NP-	333	3	Removal of P-Asserted-Identity from clause	5.3.0	5.4.0	030289 N1-
2000 00	141 15	030052	333		7 of 24.229	0.0.0	0.4.0	030310
2003-03	NP-19	NP-	334		P-CSCF general procedure corrections	5.3.0	5.4.0	N1-
0000.00	NID 40	030052	005		11 (0 () () ()	500	5.4.0	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
2003-03	NP-19	NP-	337		Usage of P-Asserted-Identity for responses	5.3.0	5.4.0	N1-
		030052						030193
2003-03	NP-19	NP-	339	2	Authorization for registration event package	5.3.0	5.4.0	N1-
2003-03	NP-10	030052 NP-	341	1	P-CSCF subscription to reg event	5.3.0	5.4.0	030285 N1-
2003-03	141-119	030052	J -1 1	['	1 -0001 Subscription to reg event	3.3.0	3.4.0	030284
2003-06	NP-20	NP-	295	4	Security agreement inclusion in SIP profile	5.4.0	5.5.0	N1-
		030275		1				030939
2003-06	NP-20	NP-	322	5	3GPP P-header inclusion in SIP profile	5.4.0	5.5.0	N1-
2003-06	NP-20	030275 NP-	332	5	Change of IP address for the UE	5.4.0	5.5.0	030938 N1-
2000-00	1.1. 20	030275	302		Change of it address for the OL	0.7.0	0.0.0	030923
2003-06	NP-20	NP-	342		Removal of the requirement for UE re-	5.4.0	5.5.0	N1-

					Change history			
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
		030275			authentication initiated by HSS			030349
2003-06	NP-20	NP- 030275	343	2	UE behaviour on reception of 420 (Bad	5.4.0	5.5.0	N1- 030552
2003-06	NP-20	NP-	347	2	Extension) message Handling of DTMF	5.4.0	5.5.0	N1-
2003-00	141 -20	030275	347	_		5.4.0	3.5.0	030551
2003-06	NP-20	NP-	348	1	Format of Tel URL in P-Asserted-Id	5.4.0	5.5.0	N1-
	0	030276				00	0.0.0	030510
2003-06	NP-20	NP-	349		Delete Note on header stripping/SDP	5.4.0	5.5.0	N1-
		030276			manipulation			030387
2003-06	NP-20	NP-	354	1	Clarifications on using DNS procedures	5.4.0	5.5.0	N1-
0000 00	NID OO	030276	0.50	1.	A 1 151	5.4.0		030520
2003-06	NP-20	NP-	356	4	Addition of procedures at the AS for SDP	5.4.0	5.5.0	N1-
2003-06	ND 20	030276 NP-	357	1	Usage of P-Associated-URI	5.4.0	5.5.0	030942 N1-
2003-00	INF-20	030276	337	'	Usage of F-Associated-ORI	5.4.0	3.3.0	030499
2003-06	NP-20	NP-	359	1	Network-initiated deregistration at UE and P-	5.4.0	5.5.0	N1-
	0	030276			CSCF	00	0.0.0	030501
2003-06	NP-20	NP-	360	2	Barred identities	5.4.0	5.5.0	N1-
		030276						030550
2003-06	NP-20	NP-	365	1	PDP contex subject to SBLP cannot be	5.4.0	5.5.0	N1-
2002.00	ND 00	030276	200	4	reused by other IMS sessions	F 4 0	<i></i>	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-	369	3	S-CSCF behavior correction to enable call	5.4.0	5.5.0	N1-
2000 00	141 20	030277	303		forwarding	0.4.0	0.0.0	030931
2003-06	NP-20	NP-	370	1	SUBSCRIBE request information stored at	5.4.0	5.5.0	N1-
		030277			the P-CSCF and S-CSCF			030521
2003-06	NP-20	NP-	371	1	Profile Tables - Transparency	5.4.0	5.5.0	N1-
		030277		1				030858
2003-06	NP-20	NP-	375	1	Profile Tables - Major Capability Corrections	5.4.0	5.5.0	N1-
2003-06	ND-20	030277 NP-	376	2	Profile Tables - Deletion of Elements not	5.4.0	5.5.0	030860 N1-
2003-00	INF-20	030277	370	_	used in 24.229	5.4.0	3.3.0	030921
2003-06	NP-20	NP-	377	1	Use of the QoS parameter 'signalling	5.4.0	5.5.0	N1-
		030277			information' for a signalling PDP context			030840
2003-06	NP-20	NP-	378	2	Deregistration of a PUID (not the last one)	5.4.0	5.5.0	N1-
0000 00	NID OO	030277	070			5.4.0		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-	380	1	Check Integrity Protection for P-Access-	5.4.0	5.5.0	N1-
2000 00	141 20	030277	000	'	Network-Info header	0.1.0	0.0.0	030881
2003-06	NP-20	NP-	381	1	PCSCF setting of Integrity protection	5.4.0	5.5.0	N1-
		030278			indicator and checking of Security Verify			030882
					header			
2003-06	NP-20	NP-	383	1	Consistent treatment of register and de-	5.4.0	5.5.0	N1-
2003-06	ND 20	030278 NP-	384	1	register Optionality of sending CK is removed	5.4.0	5.5.0	030884 N1-
2003-00	141 -20	030278	304	'	Optionality of sending Cit is removed	3.4.0	3.3.0	030885
2003-06	NP-20	NP-	385	1	Addition of note and Correction of	5.4.0	5.5.0	N1-
		030278			References regarding security associations			030886
					and registration			
2003-06	NP-20	NP-	387	1	Subscription/Registration refresh time	5.4.0	5.5.0	N1-
2002.00	ND 00	030278	200	1	Corrections to use of IV	E 4 0	E E O	030887
2003-06	INP-20	NP- 030278	388	1	Corrections to use of IK	5.4.0	5.5.0	N1- 030863
2003-06	NP-20	NP-	390		Mobile-originating case at UE	5.4.0	5.5.0	N1-
		030278						030647
2003-06	NP-20	NP-	394	2	Re-authentication procedure.	5.4.0	5.5.0	N1-
		030278			·			030917
2003-06	NP-20	NP-	395		Replacement of SIP URL with SIP URI	5.4.0	5.5.0	N1-
		030278	007	2	Night in the section of the section	5.4.0	5.5.0	030652
0000 00	NID CC			1.)	Notification about registration state	154()	1550	N1-
2003-06	NP-20	NP- 030279	397	2	Troumoutor about regionation state	0.4.0	0.0.0	030926

Dat-	TCO "	TOOD	100	Г.	Change history	01.1	N	Wo :
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
0000 00	ND CC	030279	404	4	C COCE initiated indicates of the control of	F 4 0		030848
2003-06	NP-20	NP-	404	1	S-CSCF initiated release of calls to circiut	5.4.0	5.5.0	N1-
2003-06	ND 20	030279 NP-	405	2	switched network Supported Integrity algorithms	5.4.0	5.5.0	030873 N1-
2003-06	INP-20	030279	405	2	Supported integrity algorithms	5.4.0	5.5.0	030927
2003-06	ND 20	NP-	407	1	RFC 3524, Single Reservation Flows	5.4.0	5.5.0	N1-
2003-06	INP-20	030279	407	'	RFC 3524, Single Reservation Flows	5.4.0	5.5.0	030851
2003-06	ND 20	NP-	410	1	Clarification of the S-CSCF's handling of the	5.4.0	5.5.0	N1-
2003-06	INF-20	030279	410		P-access-network-info header	5.4.0	5.5.0	030868
2003-06	ND 20	NP-	411	2	Port numbers in the RR header entries	5.4.0	5.5.0	N1-
2003-06	INF-20	030279	411	2	Port numbers in the RR neader entities	5.4.0	5.5.0	030941
2003-06	ND 20	NP-	412	2	Registration abnormal cases	5.4.0	5.5.0	N1-
2003-00	INF-20	030279	412	2	Registration abriornal cases	3.4.0	5.5.0	030928
2003-06	NID-20	NP-	415		Minor correction to section 5.4.5.1.2	5.4.0	5.5.0	N1-
2003-00	INF-20	030280	413		Willion Correction to Section 5.4.5.1.2	3.4.0	5.5.0	030720
2003-06	NP-20	NP-	417	1	Introduction of RTCP bandwidth	5.4.0	5.5.0	N1-
2003-00	111 -20	030280	1717	'	linitoddciion of KTOL bandwidin	3.4.0	3.3.0	030872
2003-06	NP-20	NP-	418	1	Registratin Event - Shortend	5.4.0	5.5.0	N1-
2003-00	141 -20	030280	710	'	Tregistratiff Everit - Offorterio	3.4.0	5.5.0	030844
2003-06	NP-20	NP-	419	1	HSS / S-CSCF text relating to user	5.4.0	5.5.0	N1-
_555 00	20	030280	1,13	1'	deregistration	0.7.0	0.0.0	030845
2003-06	NP-20	NP-	421		Handling of unknown methods at the P-	5.4.0	5.5.0	N1-
_555 55	20	030280	'- '		CSCF	3. 7.0	0.0.0	030743
2003-06	NP-20	NP-	422	1	Definitions and abbreviations update	5.4.0	5.5.0	N1-
2000 00	111 20	030280	122	'	Dominiono una abbreviatione apaate	0.1.0	0.0.0	030870
2003-06	NP-20	NP-	423		Removal of hanging paragraph	5.4.0	5.5.0	N1-
2000 00	141 20	030280	720		Tremoval of Hariging paragraph	0.4.0	0.0.0	030752
2003-06	NP-20	NP-	424		Access network charging information	5.4.0	5.5.0	N1-
_000 00	20	030280	1		7 toose flotwork oranging information	0	0.0.0	030753
2003-06	NP-20	NP-	425	1	UE procedure tidyup	5.4.0	5.5.0	N1-
	20	030280	1.20	'	or procedure mayap	0	0.0.0	030871
2003-06	NP-20	NP-	426		P-CSCF procedure tidyup	5.4.0	5.5.0	N1-
	0	030281	0		Procedure may ap	00	0.0.0	030755
2003-06	NP-20	NP-	427		I-CSCF procedure tidyup	5.4.0	5.5.0	N1-
	•	030281			The second secon			030756
2003-06	NP-20	NP-	428		S-CSCF procedure tidyup	5.4.0	5.5.0	N1-
		030281						030757
2003-06	NP-20	NP-	429		BGCF procedure tidyup	5.4.0	5.5.0	N1-
		030281						030758
2003-06	NP-20	NP-	430		AS procedure tidyup	5.4.0	5.5.0	N1-
		030281						030759
2003-06	NP-20	NP-	431		MRFC procedure tidyup	5.4.0	5.5.0	N1-
		030281						030760
2003-06	NP-20	NP-	434	1	SDP procedure tidyup	5.4.0	5.5.0	N1-
		030281			·			030852
2003-06	NP-20	NP-	438	2	Profile Tables – Further Corrections	5.4.0	5.5.0	N1-
		030281						030935
2003-06	NP-20	NP-	439	3	AS's subscription for the registration state	5.4.0	5.5.0	N1-
		030281			event package	1		030940
2003-06	NP-20	NP-	440		Temporary Public User Identity in re- and de-	5.4.0	5.5.0	N1-
		030281			REGISTER requests			030792
2003-09	NP-21	NP-	444	2	All non-REGISTER requests must be	5.5.0	5.6.0	N1-
		030412			integrity protected	ļ		031328
2003-09	NP-21	NP-	445		Download of all service profiles linked to	5.5.0	5.6.0	N1-
		030412	1		PUID being registered and implicitly			031010
		1	1.		registered	<u> </u>	1_	1
2003-09	NP-21	NP-	448	3	Authentication at UE	5.5.0	5.6.0	N1-
		030412	1.	1		<u> </u>	1_	031326
2003-09	NP-21	NP-	449	1	Nework authentication failure at the UE	5.5.0	5.6.0	N1-
		030412				<u> </u>		031242
2003-09	NP-21	NP-	451	3	Handling of security association	5.5.0	5.6.0	N1-
		030412	1	1		<u> </u>		031327
2003-09	NP-21	NP-	452	1	Re-authentication timer at S-CSCF	5.5.0	5.6.0	N1-
	1	030412				1	1	031274

		_			Change history			
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New	WG doc
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	001000
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-	468		Update of references	5.5.0	5.6.0	N1- 031094
2003-09	NP-21	030413 NP-	470	1	Adding P-Asserted-Identity headers to NE	5.5.0	5.6.0	N1-
2003-09	NP-21	030414 NP-	479	1	initiated subscriptions Replace USIM by ISIM for user identity	5.5.0	5.6.0	031314 N1-
2003-09	NP-21	030414 NP-	481	1	storage 24.229 R5 CR: Corrections to Profile Tables	5.5.0	5.6.0	031247 N1-
2003-09	NP-21	030414 NP-	482		24.229 R5 CR: Setting of SUBSCRIBE	5.5.0	5.6.0	031248 N1-
2003-09	NP-21	030414 NP-	483	3	exipiration time 24.229 R5 CR: Alignment of IMS	5.5.0	5.6.0	031140 N1-
2003-12	NP-22	030414 NP-	485	1	Compression with RFC 3486 INVITE dialog amendments in profile	5.6.0	5.7.0	031335 N1-
2003-12	NP-22	030476 NP-	495	1	P-Asserted-Identity in SUBSCRIBE requests	5.6.0	5.7.0	031358 N1-
2003-12	NP-22	030476 NP-	502	2	Update of HSS information at deregistration	5.6.0	5.7.0	031631 N1-
2003-12	NP-22	030476 NP-	508		Reference corrections	5.6.0	5.7.0	031719 N1-
2003-12	NP-22	030476 NP-	523	2	Correct use of RAND during re-	5.6.0	5.7.0	031393 N1-
2003-12		030477 NP-	525	1	synchronisation failures Correction to description or RES/XRES	5.6.0	5.7.0	031711 N1-
2003-12		030478 NP-	530	3	usage Corrections on ICID for REGISTER	5.6.0	5.7.0	031616
2003-12		030581 NP-	542	1	Correction of user initiated re-registration	5.6.0	5.7.0	N1-
2003-12		030478 NP-			-			031618
		030478	550	1	IMS trust domain in Rel 5	5.6.0	5.7.0	N1- 031621
2003-12		NP- 030478	555	1	P-CSCF and UE handling of Security Associations	5.6.0	5.7.0	N1- 031623
2003-12		NP- 030478	565		Sending challenge	5.6.0	5.7.0	N1- 031579
2003-12		NP- 030480	567	2	Reg-await-auth timer value	5.6.0	5.7.0	N1- 031715
2003-12		NP- 030480	570	1	Network initiated deregistration	5.6.0	5.7.0	N1- 031706
2004-03		NP- 040027	367	6	Completion of major capabilities table in respect of privacy	5.7.0	5.8.0	N1- 040405
2004-03	NP-23	NP- 040027	498	5	P-CSCF integrity protection	5.7.0	5.8.0	N1- 040499
2004-03	NP-23	NP- 040027	585	1	Network-initiated re-authentication	5.7.0	5.8.0	N1- 040392
2004-03	NP-23	NP- 040027	591	1	Integrity protected correction	5.7.0	5.8.0	N1- 040399
2004-03	NP-23	NP- 040027	599	2	Handling of record-route in target refresh and subsequent request	5.7.0	5.8.0	N1- 040480

-	T00 "	ITO 0 D	100	1_	Change history		1	lwo i
Date	TSG #	TSG Doc.	CR 607	Rev	Subject/Comment	Old	New	WG doc
2004-03	NP-23	NP- 040134		3	Unprotected deregistration	5.7.0	5.8.0	
2004-03	NP-23	NP- 040029	609		Sending authentication challenge	5.7.0	5.8.0	N1- 040330
2004-03	NP-23	NP- 040029	614	1	Support of MESSAGE (Profile Tables)	5.7.0	5.8.0	N1- 040465
2004-06	NP-24	NP- 040189	630	1	Missing statements regarding P-Charging- Function-Addresses header	5.8.0	5.9.0	N1- 040986
2004-06	NP-24	NP- 040189	641	3	Syntax of the extension to the P-Charging- Vector header field	5.8.0	5.9.0	N1- 041099
2004-06	NP-24	NP- 040189	647	1	Correction of reception of media authorization token	5.8.0	5.9.0	N1- 040993
2004-06	NP-24	NP-	648	1	Revisions due to published version of draft-	5.8.0	5.9.0	N1-
2004-09	NP-25	040189 NP-			ietf-sipping-reg-event	5.9.0	5.10.0	040991 N1-
0004.00	ND OF	040381 NP-	701		NOTIFY requests Syntax correction for the P-Charging-Vector	500	5.40.0	041639 N1-
2004-09	NP-25	040385	672	1	header	5.9.0	5.10.0	041537
2004-09	NP-25	NP- 040385	679	1	Missing value for the event attribute within the <contact> element of NOTIFY body</contact>	5.9.0	5.10.0	N1- 041541
2004-09	NP-25	NP- 040385	694	1	Correction to condition for removal of the P-Access- Network-Info Header	5.9.0	5.10.0	N1- 041552
2004-09	NP-25	NP-			Network initiated deregistration upon UE	5.9.0	5.10.0	N1-
2004-12	ND 26	040385 NP-	681	2	roaming and registration to a new network	5.10.0	5.11.0	041628 N1-
2004-12	INP-20	040502	722	1	Correction Term IOI handling	5.10.0	5.11.0	041955
2004-12	NP-26	NP-			Request handling in S-CSCF originating	5.10.0	5.11.0	N1-
		040502	724	1	case			041957
2004-12	NP-26	NP-	706	1	Request handling in S-CSCF - terminating	5.10.0	5.11.0	N1- 041959
		040502	726	'	case			
2004-12	NP-26	NP- 040502	737	1	Population of Via header when using REGISTER method	5.10.0	5.11.0	N1- 041961
2004-12	NP-26				Network-initiated deregistration for the old	5.10.0	5.11.0	
200112	20	NP-			contact information of a roaming UE	0.10.0	0.11.0	N1-
		040502	754	1	registered in a new network			042091
2004-12	NP-26	NP- 040502	764	1	Interaction between S-CSCF and HSS in Network initiated deregistration procedure	5.10.0	5.11.0	N1- 041965
2004-12	NP-26	NP- 040502	767	1	Downloading of user profile	5.10.0	5.11.0	N1- 042102
2005-01					Fix Word problem	5.11.0	5.11.1	
2005-03	NP-27	NP-	+			5.11.1	5.12.0	N1-
2000 00	2.	050069	784		Deregistration effect on active sessions	0	0.12.0	050051
2005-03	NP-27	NP-	005		Han of minimal dialogs in 1977 at AO	5.11.1	5.12.0	N1-
		050069	805	1	Use of original dialog identifier at AS			050291
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
2005.00	ND CZ	ND				F 44 4	F 40.0	NA
2005-03	NP-27	NP- 050069	809	1	IOI storage at MGCF	5.11.1	5.12.0	N1- 050295
2005-03	NP-27				Filter criteria matching and generation of	5.11.1	5.12.0	
		NP-			third-party REGISTER request for			N1-
		050069	839		network-initiated deregistration			050220
		CP-050059	869	1	Port 5060	 	+	C1-050673

D-(T00 "	TOCO	105		Change history			lwc :
Date 2005-06	TSG #	TSG Doc. CP-050059	CR 878	Rev	Subject/Comment Correction Reg-Await-Auth Timer	Old	New	WG doc C1-050521
2005-06	CP-28	CP-050059	878			5.12.0	5.13.0	C1-050521
2005-06	CP-28	CP-050059	880		Security Association In P-CSCF	5.12.0	5.13.0	C1-050523
2005-06	CP-28				SIP headers storage for P-CSCF initiated session		51.0.0	
		CP-050059	922		release	5.12.0	5.13.0	C1-050776
2005-06	CP-28	OD 050050	0.4.7		Call-Id mismatch in the protected REGISTER			04.050005
		CP-050059	917	1	when reg-await-auth timer is running	5.12.0	5.13.0	C1-050685
2005-06	CP-28	CP-050059	920	1	Correction of error in the specification of the extension to Authorization header			C1-050688
						5.12.0	5.13.0	
2005-06	CP-28	CP-050059	859	2	S-CSCF failure	5.12.0	5.13.0	C1-050780
2005-06	CP-28	CP-050059	885	2	Handling of P-Associated URI header			C1-050782
2005-06	CP-28	CP-050059	906	2	Clarification to the procedures at the I-CSCF	5.12.0	5.13.0	C1-050784
		CP-050355	928	1	Correction Profile Table A.119	5.12.0	5.13.0	C1-051059
2005-09	CP-29			'		5.13.0	5.14.0	
2005-09	CP-29	CP-050355	944		Public User identity in 3rd party REG	5.13.0	5.14.0	C1-050904
2005-09	CP-29	CP-050355	963		Optional ccf			C1-050984
2005-09	CP-29				Removal of Access Network Charging Information	5.13.0	5.14.0	
	0. 20	CP-050355	983		by the S-CSCF	E 12 0	E 14 0	C1-051082
2005-09	CP-29	CP-050355	984		Contact header in REGISTER requests	5.13.0	5.14.0	C1-051175
2005-12	CP-30	CP-050538	1047		Replace 'originated' with 'terminated'	5.13.0	5.14.0	C1-051477
						5.14.0	5.15.0	
2005-12	CP-30	CP-050538	1010	1	Correction to section 5.4.3.2 of TS 24.229	5.14.0	5.15.0	C1-051561
2005-12	CP-30	CP-050538	1044	2	Mobile originating call related requests			C1-051666
2005-12	CP-30	CP-050538	1024		Handling of P-Charging-Function-Address	5.14.0	5.15.0	C1-051422
2006-03		CP-060106	1112	1	IMS AKA - content of initial authentication header	5.14.0	5.15.0	C1-060448
	CP-31					5.15.0	5.16.0	
2006-03	CP-31	CP-060106	1115	1	IMS AKA - SQN resync clarifications	5.15.0	5.16.0	C1-060450
2006-03	CD 24	CP-060107	1140	1	Support of call forwarding at the S-CSCF			C1-060461
2006-03	CP-31	CP-060152	1146	2	UE processing 305 (Use Proxy)	5.15.0	5.16.0	C1-060505
	CP-31	CP-060107	1159	1	DHCPv6 options for Domain Name Servers	5.15.0	5.16.0	C1-060454
2006-03	CP-31				•	5.15.0	5.16.0	
2006-03	CP-31	CP-060107	1162	1	Clarifications on P-CSCF discovery	5.15.0	5.16.0	C1-060457
2006-03	-	OD 000400	4405		Removal of Warning header non-compliance with			04 000000
	CP-31	CP-060106	1185	_	RFC 3261	5.15.0	5.16.0	C1-060326
2006-03		CP-060106	1202		Syntax and operation for Security-Client, Security-Server and Security-Verify headers			C1-060385
	CP-31				, ,	5.15.0	5.16.0	
2006-03	CP-31	CP-060107	1220	-	Reference Update of TS24.229	5.15.0	5.16.0	C1-060484
2006-06		CP-060230	1288	2	Realm Parameter Handling	5.16.0		
2006-06	CP-32	CP-060262	1307	1	Hiding correction		5.17.0	C1-061043
2006-06	CP-32	CP-060262	1304	2	3rd-party registration	5.16.0	5.17.0	C1-061096
	CP-32				. , ,	5.16.0	5.17.0	
2006-06	CP-32	CP-060262	1301	2	One private identity one contact	5.16.0	5.17.0	C1-061093
2006-06	CP-32	CP-060262	1272	1	Re-authentication during deregistration			C1-060961
2006-06		CP-060265	1310		I-CSCF registration procedure correction	5.16.0	5.17.0	C1-060827
2006-09	CP-32				"Response" value in unprotected Register	5.16.0	5.17.0	
2000-08		CP-060452	1473	2	requests			C1-061843
	CP-33					5.17.0	5.18.0	

	Change history							
Date	TSG #	TSG Doc.	CR		Subject/Comment	Old	New	WG doc
2006-09		CP-060452	1403	1	Removal of Editor's notes in 24.229, rel-5			C1-061729
0000.00	CP-33				() () () () ()	5.17.0	5.18.0	
2006-09		CP-060452	1459	4	Correction of Realm Parameter Handling for S- CSCF procedures			C1-061730
	CP-33	CP-060452	1459	1	CSCF procedures	5.17.0	5.18.0	C1-061730
2006-09	01 33	CP-060452	1465		SDP reference revision	0.17.0	0.10.0	C1-061655
2000 00	CP-33	01 000402	1400		Telefelloc revision	5.17.0	5.18.0	01 001000
2006-09		CP-060452	1476	1	Enabling Rel-5 UE to set up sendonly sessions			C1-061737
	CP-33					5.17.0	5.18.0	
2007-06					THIG processing correction to ensure conformity			
		CP-070448	1777	2	to RFC 3261			
	CP-36					5.18.0	5.19.0	
2007-09	CP-37	CP-070578	1808		Integrity param in De- and ReREGISTER	5.19.0	5.20.0	C1-071570
2007-09					Correction of the Authorization Header in the			
2007-09	CP-37	CP-070578	1785	1	Profile Table	5.19.0	5.20.0	C1-072082
	01 -57	01-070370	1703	'	Tronie rabie	3.13.0	3.20.0	01-072002
2007-09	CP-37	CP-070579	1902	2	Clarification of DTD	5.19.0	5.20.0	C1-072147
2007-12	CP-38	CP-070785	1958	1	Authenticating with AKAv1-MD5	5.20.0	5.21.0	C1-072530
2007-12	CP-38	CP-070785	2038	1	Corrections for re-authenticating user	5.20.0	5.21.0	C1-072550
0007.40	00.00	00 070705	0400		0 " , PEO 0000 , ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;	5.00.0	5.04.0	04.070045
2007-12	CP-38	CP-070785	2108		Corrections to RFC 3329 entries in profile	5.20.0	5.21.0	C1-072915
2007-12	CP-38	CP-070785	2112		Proxy profile corrections	5.20.0	5.21.0	C1-072919
2007-12	CF-30	CF-070763	2112		Froxy profile corrections	3.20.0	3.21.0	01-072919
2007-12	CP-38	CP-070785	2046	5	Introduction of versioning and conventions	5.20.0	5.21.0	C1-072986
2007 12	0. 00	0. 0.0.00	20.0		Third decision of versioning and conventions	0.20.0	0.21.0	0.0.2000
2007-12					Correction of 3GPP IM CN subsystem XML		5.21.0	
	CP-38	CP-070870	2094	4	handling	5.20.0		C1-073167
2008-09	CP-41	CP-080514	2311	1	Correction on identifiers distinguishing the dialog	5.21.0	5.22.0	C1-082605
	00.44	05.00511						01.000.00
2008-09	CP-41	CP-080514	2387		One contact address per UE	5.21.0	5.22.0	C1-083503
2009-09	CP-45	CP-090644	2621	3	Inconsistency between text and XML schema	5.22.0	5.23.0	C1-093705
2009-09	OF-45	CF-090044	2021	٥	Iniconsistency between text and AME SCHEMA	3.22.0	5.23.0	01-093/05
2010-12	CP-50	CP-100875	3372	2	Codec and DTMF correction	5.23.0	5.24.0	-
				_		0.20.0	0.2	
2011-09	CP-53	CP-110648	3694		"P-Visited-Network-ID" correction	5.24.0	5.25.0	C1-112998
			<u> </u>					
2012-03	CP-55	CP-120093	3910	1	Geo-Redundancy Registration	5.25.0	5.26.0	C1-120550

History

		Document history
V5.1.0	June 2002	Publication
V5.2.0	September 2002	Publication
V5.3.0	December 2002	Publication
V5.4.0	March 2003	Publication
V5.5.0	June 2003	Publication
V5.6.0	September 2003	Publication
V5.7.0	December 2003	Publication
V5.8.0	March 2004	Publication
V5.9.0	June 2004	Publication
V5.10.0	September 2004	Publication
V5.11.1	January 2005	Publication
V5.12.0	March 2005	Publication
V5.13.0	June 2005	Publication
V5.14.0	September 2005	Publication
V5.15.0	December 2005	Publication
V5.16.0	March 2006	Publication
V5.17.0	June 2006	Publication
V5.18.0	September 2006	Publication
V5.19.0	June 2007	Publication
V5.20.0	October 2007	Publication
V5.21.0	January 2008	Publication
V5.22.0	October 2008	Publication
V5.23.0	October 2009	Publication
V5.24.0	March 2011	Publication
V5.25.0	November 2011	Publication
V5.26.0	March 2012	Publication