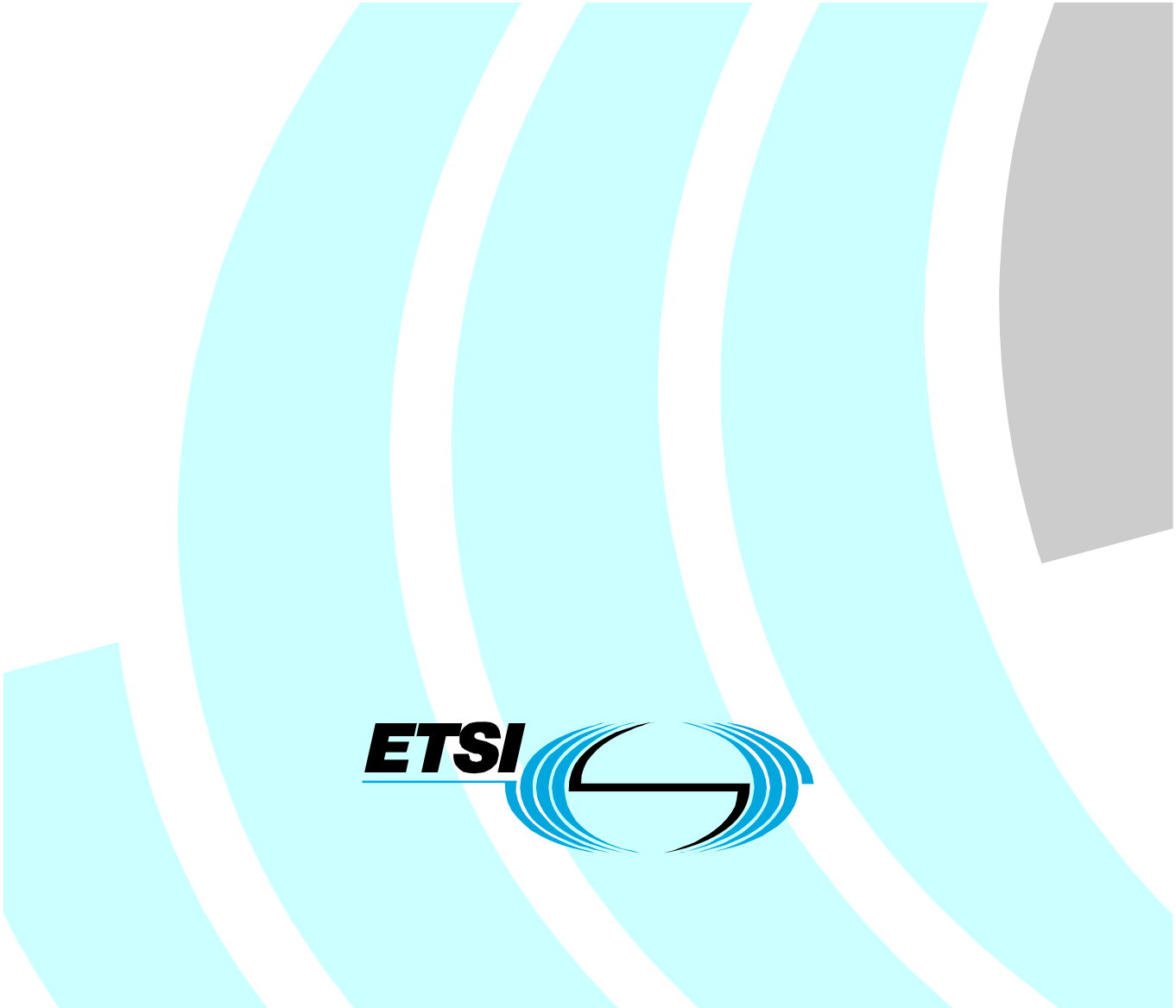
ETSI ES 283 003 V2.5.1 (2008-04)

ETSI Standard

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3

[3GPP TS 24.229 [Release 7], modified]



Reference
RES/TISPAN-03120-NGN-R2

Keywords
endorsement, IP, multimedia, profile

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

Contents

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://webapp.etsi.org/IPR/home.asp).

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 ETSI Standard (ES) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document provides the ETSI TISPAN endorsement of 3GPP TS 24.229 [1]: "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 7)" in line with the requirements of TISPAN NGN.

The present document together with the endorsed document provides the necessary SIP/SDP specifications for supporting TISPAN Release 2 requirements, with the exception of some of the features required for Business Trunking services (e.g. procedures for handling Wildcarded Public User Identities) and IPTV services (e.g. SDP extensions). Modifications required in support of these features are expected to be included as essential corrections to the present document.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] 3GPP TS 24.229 (V7.9.0): "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[2] ETSI TS 183 008: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR); Protocol specification".

[3] ETSI TS 183 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); Protocol specification".

Endorsement notice

The present document endorses 3GPP TS 24.229 (V7.9.0): "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 (Release 7)" [1].

The present document shows the modifications, additions and deletions through the use of underlined and strikethrough text.

For the purpose of the present document clause 1 of [1] applies.

For the purpose of the present document clause 3 of [1] applies except for clause 3.2, which is replaced by the appropriate clause in clause 3 of the present document.

For the purpose of the present document clause 4 of [1] applies, except for clauses 4.1 and 4.2, which are replaced by the appropriate clauses in clause 4 of the present document.

For the purpose of the present document clause 5 of [1] applies, except for clauses 5.1.1.1A, 5.1.1.2, 5.1.1.3, 5.1.1.4, 5.1.1.5.1, 5.1.1.5.2, 5.1.1.5A, 5.1.1.6, 5.1.1.7, 5.1.2A.1, 5.1.2.A2, 5.2.1, 5.2.2, 5.2.5.1, 5.2.5.2, 5.2.6.2, 5.2.6.3, 5.2.6.4, 5.2.7.2, 5.2.7.3, 5.2.8.1.1, 5.2.8.1.2, 5.2.8.1.4, 5.2.8.3, 5.2.10.1, 5.2.10.3, 5.4.1.1, 5.4.1.2, 5.4.1.2.1, 5.4.1.3, 5.4.1.4, 5.4.1.6, 5.4.1.7, 5.4.3.2, 5.4.3.3 and 5.10.6, which are replaced by the appropriate clauses in clause 5 of the present document. In addition clauses 5.1.1.1B, 5.1.1.2A, 5.1.1.4A, 5.1.1.5.1A, 5.1.1.5.1B, 5.1.1.6A, 5.2.2A and 5.4.1.2A.1 are added.

For the purpose of the present document clause 6 of [1] applies, except for clauses 6.1.1 and 6.2 , which are replaced by the appropriate clauses in clause 6 of the present document.

For the purpose of the present document clause 7 of [1] applies, except for clause 7.2A.4, which is replaced by the appropriate clause in clause 7 of the present document.

For the purpose of the present document clause 9 of [1] applies.

For the purpose of the present document annex A of [1] applies, except for clauses A.2.1.2, A.2.1.4.7, A2.1.4.12, A.2.2.4.7 and A.3.2.1 which are replaced by the appropriate clauses in annex A of the present document.

For the purpose of the present document annex F of [1] is replaced with annex F of the present document.

For the purpose of the present document annex G of [1] is replaced with annex G of the present document.

For the purpose of the present document annex I of [1] applies.

For the purpose of the present document annex J of [1] applies, except for clauses J.1 and J.2 which are replaced by the appropriate clauses in annex J of the present document. In addition clause J.9A is added.

For the purpose of the present document annex F of [1] applies, except for clauses F.4.1 and F.4.2 which are replaced as indicated in the appropriate clauses in annex F of the present document.

For the purpose of the present document annex F of [1] applies with the addition of clause F.4A.

Global modifications to 3GPP TS 24.229

The references in clause 2 of [1] should be replaced as shown in table 1.

Table 1

References in 3GPP TS 24.229 [1]	Replaced references
[2] 3GPP TS 23.002: "Network architecture".	ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture" (note 1)
	ETSI ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 2" (note 1)
[4A] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".	(note 2)

References in 3GPP TS 24.229 [1]	Replaced references
[4B] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency session; Stage 2".	ETSI TS 182 009: “Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Architecture to support emergency communication from citizen to authority” (note 1)
[4C] 3GPP TS 23.122: "Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode".	(note 2)
[5] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".	(note 2)
[6] 3GPP TS 23.221: "Architectural requirements".	(note 2)
[7] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".	ETSI TS 182 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Stage 2 description"
[8] 3GPP TS 24.141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".	ETSI ES 283 030: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Presence Service Capability; Protocol Specification [3GPP TS 24.141 V7.0.0, modified and OMA-TS-Presence_SIMPLE-V1_0, modified]" (note 1)
[10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".	ETSI TS 181 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services and Capabilities Requirements” (note 1)
[10A] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services".	(note 2)
[11A] 3GPP TS 29.162: "Interworking between the IM CN subsystem and IP networks".	ETSI TS 183 021: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Endorsement of 3GPP TS 29.162 Interworking between IM CN Sub-system and IP networks" (note 1)
[11B] 3GPP TS 29.163: "Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks".	ETSI ES 283 027: “Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Endorsement of the SIP-ISUP Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks [3GPP TS 29.163 (Release 7), modified]“ (note 1)
[14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".	ETSI TS 183 033: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia; Diameter based protocol for the interfaces between the Call Session Control Function and the User Profile Server Function/Subscription Locator Function; Signalling flows and protocol details [3GPP TS 29.228 V6.8.0 and 3GPP TS 29.229 V6.6.0, modified]" (note 1)
[15] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".	ETSI TS 183 033: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia; Diameter based protocol for the interfaces between the Call Session Control Function and the User Profile Server Function/Subscription Locator Function; Signalling flows and protocol details [3GPP TS 29.228 V6.8.0 and 3GPP TS 29.229 V6.6.0, modified]" (note 1)
[16] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".	ETSI ES 282 010: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Charging (Endorsement of 3GPP TS 32.240 Release 7, 3GPP TS 32.260 Release 7, 3GPP TS 32.297 Release 7, 3GPP TS 32.298 Release 7 and 3GPP TS 32.299 Release 7 modified)" (note 1)
[17] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".	ETSI ES 282 010: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Charging [Endorsement of 3GPP TS 32.240 Release 7, 3GPP TS 32.260 Release 7, 3GPP TS 32.297 Release 7, 3GPP TS 32.298 Release 7 and 3GPP TS 32.299 Release 7modified]" (note 1)
[19] 3GPP TS 33.203: "Access security for IP based services".	(note 2)
[67] draft-rosenberg-sipping-acr-code-00 (November 2005): "Rejecting Anonymous Requests in the Session Initiation Protocol (SIP)".	New reference. Editor's note: The document cannot be formally referenced until it is published as an RFC (note 1)

References in 3GPP TS 24.229 [1]	Replaced references
[68] draft-jennings-sip-voicemail-uri-05 (November 2005): "Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)".	IETF RFC 4458: "Session Initiation Protocol (SIP) URIs for Applications such as Voicemail and Interactive Voice Response (IVR)" (note 1)
[85] 3GPP2 C.S0005-D (March 2004): "Upper Layer (Layer 3) Signalling Standard for cdma2000 Standards for Spread Spectrum Systems".	(note 2)
[86] 3GPP2 C.S0024-A v1.0 (April 2004): "cdma2000 High Rate Packet Data Air Interface Standard".	(note 2)
[87] ITU-T Recommendation J.112, "Transmission Systems for Interactive Cable Television Services"	(note 2)
[88] PacketCable Release 2 Technical Report, PacketCable™ Architecture Framework Technical Report, PKT-TR-ARCH-FRM.	(note 2)
NOTE 1: The reference in [1] is replaced by the document listed on the right column. This replacement is applicable to all occurrences of the reference throughout the present endorsement.	
NOTE 2: The reference in [1] contains 3GPP or 3GPP2 or cable specific requirements and is not generally applicable to the present endorsement.	

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, clause 3.1 of [1] applies.

3.2 Abbreviations

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

1xx	A status-code in the range 101 through 199, and excluding 100
2xx	A status-code in the range 200 through 299
AAA	Authentication, Authorization and Accounting
AS	Application Server
APN	Access Point Name
AUTN	Authentication TokeN
B2BUA	Back-to-Back User Agent
BGCF	Breakout Gateway Control Function
c	conditional
BRAS	Broadband Remote Access Server
CCF	Charging Collection Function
CDF	Charging Data Function
CDR	Charging Data Record
CK	Ciphering Key
CN	Core Network
CPC	Calling Party Category
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOCSIS	Data Over Cable Service Interface Specification
DTD	Document Type Definition
EC	Emergency Centre
ECF	Event Charging Function
E-CSCF	Emergency CSCF
FQDN	Fully Qualified Domain Name
GCID	GPRS Charging Identifier
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GRUU	Globally Routable User agent URI

HPLMN	Home PLMN
~~HSS~~	~~Home Subscriber Server~~
i	irrelevant
IARI	IMS Application Reference Identifier
IBCF	Interconnection Border Control Function
I-CSCF	Interrogating CSCF
ICID	IM CN subsystem Charging Identifier
ICSI	IMS Communication Service Identifier
IK	Integrity Key
IM	IP Multimedia
IMS	IP Multimedia ~~core network~~ Subsystem
IMS-ALG	IMS Application Level Gateway
IMSI	International Mobile Subscriber Identity
IOI	Inter Operator Identifier
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
IPsec	IP security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISC	IP Multimedia Subsystem Service Control
ISIM	IM Subscriber Identity Module
IWF	Interworking Function
I-WLAN	Interworking – WLAN
LRF	Location Retrieval Function
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
n/a	not applicable
NAI	Network Access Identifier
NA(P)T	Network Address (and Port) Translation
NASS	Network Attachement Subsystem
NAT	Network Address Translation
o	optional
OCF	Online Charging Function
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy CSCF
PDG	Packet Data Gateway
PDP	Packet Data Protocol
PDU	Protocol Data Unit
PIDF-LO	Presence Information Data Format Location Object
PLMN	Public Land Mobile Network
PSAP	Public Safety Answering Point
PSI	Public Service Identity
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAND	RANDom challenge
RES	RESponse
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
S-CCF	Serving CSCF
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
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	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UDVM	Universal Decompressor Virtual Machine
UPSF	User Profile Server Function
USIM	Universal Subscriber Identity Module
VPLMN	Visited PLMN
WLAN	Wireless Local Area Network
x	prohibited
xDSL	Digital Subscriber Line (all types)
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 Ma reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk 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 Ma reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Mm reference point, the Mr reference point, the Mw reference point and the ISC reference point are defined in 3GPP TS 23.002 [2].

- 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 as described in the annexes, e.g. GPRS specific procedures described in subclause B.2.2.

- 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, 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-CCF 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-CCF shall provide the UA role with the additional capabilities, as follows:

  a) the S-CCF shall also act as a registrar. When acting as a registrar, or for the purposes of executing a third-party registration, the S-CCF shall provide the UA role;

  b) as the notifier of event information the S-CCF shall provide the UA role;

c) when providing a messaging mechanism by sending the MESSAGE method, the S-CCF shall provide the UA role; and

d) when performing S-CCF initiated dialog release the S-CCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.

- The MGCF shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.5, and with the exceptions and additional capabilities to SDP as described in subclause 6.4.

- The BGCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.6.

- The AS, acting as terminating UA, or redirect server (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.1), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.2, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.

- The AS, acting as originating UA (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.2), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.3, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.

- The AS, acting as a SIP proxy (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.3), shall 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.

- The IBCF shall provide the proxy role, with the exceptions and additional capabilities to SIP as described in subclause 5.10, and with the exceptions and additional capabilities to SDP as described in subclause 6.6. If the IBCF provides an application level gateway functionality, then the IBCF shall provide the UA role, with the exceptions and additional capabilities to SIP as described in subclause 5.10, and with the exceptions and additional capabilities to SDP as described in subclause 6.6. If the IBCF provides screening functionality, then the IBCF may provide the UA role, with the exceptions and additional capabilities to SIP as described in subclause 5.10.

- The E-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.11.

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

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 5.2 the P-CSCF implements proxy requirements. Despite being a B2BUA a P-CSCF does not implement UA requirements from the IETF RFCs, except as indicated in this specification, e.g., relating to registration event subscription.

NOTE 4: Except as specified in clause 5 or otherwise permitted in RFC 3261, the functional entities providing the proxy role are intended to be transparent to data within received requests and responses. Therefore these entities do not modify message bodies. If local policy applies to restrict such data being passed on, the functional entity has to assume the UA role and reject a request, or if in a response and where such procedures apply, to pass the response on and then clear the session using the BYE method.

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

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

4.2 URI and address assignments

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

1) I-CSCFs used in registration are allocated SIP URIs. Other IM CN subsystem entities may be allocated SIP URIs. For example sip:pcscf.home1.net and sip:<impl-specific-info>@pcscf.home1.net are valid SIP URIs. If the user part exists, it is an essential part of the address and shall not be omitted when copying or moving the address. How these addresses are assigned to the logical entities is up to the network operator. For example, a single SIP URI may be assigned to all I-CSCFs, and the load shared between various physical boxes by underlying IP capabilities, or separate SIP URIs may be assigned to each I-CSCF, and the load shared between various physical boxes using DNS SRV capabilities.

2) All IM CN subsystem entities are allocated IP addresses. For systems providing access to IMS using a fixed broadband network, any IM CN Subsystem entities can be allocated IPv4 only, IPv6 only or both IPv4 and IPv6 addresses. Otherwise, systems shall support IP addresses as 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. Where no ISIM application is present but USIM is present, the private user identity is derived (see subclause 5.1.1.1A). This private user identity is available to the SIP application within the UE. For UEs, where neither ISIM application nor USIM are present, the private user identity is available to the UE via other means (see subclause 5.1.1.1B).

NOTE 1: The SIP URIs can be resolved by using any of public DNSs, private DNSs, or peer-to-peer agreements.

4) The subscriber is allocated one or more public user identities by the home network operator. The public user identity shall take the form of SIP URI as specified in RFC 3261 [26] or tel URI as specified in RFC 3966 [22]. At least one of the public user identities is a SIP URI and it is stored within the ISIM application, if ISIM application is present. Where no ISIM application is present but USIM is present, the UE derives a temporary public user identity (see subclause 5.1.1.1A). All registered public user identities are available to the SIP application within the UE, after registration.

5) If the UE supports GRUU (see table A.4, item A.4/53), then it shall have an Instance ID, in conformance with the mandatory requirements for Instance IDs specified in draft-ietf-sip-gruu [93] and draft-ietf-sip-outbound [92].

6) For each tel URI, there is at least one alias SIP URI in the set of implicitly registered public user identities that is used to implicitly register the associated tel URI.

7) The public user identities may be shared across multiple UEs. A particular public user identity may be simultaneously registered from multiple UEs that use different private user identities and different contact addresses. When reregistering and deregistering a given public user identity and associated contact address, the UE will use the same private user identity that it had used during the initial registration of the respective public user identity and associated contact address. If the tel URI is a shared public user identity, then the associated alias SIP URI is also a shared public user identity. Likewise, if the alias SIP URI is a shared public user identity, then the associated tel URI is also a shared public user identity.

8) For the purpose of access to the IM CN subsystem, UEs 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). In the particular case of UEs accessing the IMS using a fixed broadband interconnection, UEs can be allocated IPv4 only, IPv6 only or both IPv4 and IPv6 addresses.

9) For the purpose of emergency service, the UE shall use at least an emergency public user identity, which is a SIP URI derived as specified in 3GPP TS 23.003 [3] and an associated tel URI.

10) An ICSI value coded as a URN (as specified in subclause 7.2A.8.2), may be included in a P-Preferred-Service header field by the UE as specified in draft-drage-sipping-service-identification [121]. The S-CCF and third party AS need to have a means for the purposes of authorization to obtain and understand the media and service characteristic related to the subscribed service as identified by the ICSI value.

4.2A Transport mechanisms

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

NOTE 1: Support of SCTP as specified in RFC 4168 [96] is optional for IM CN subsystem entities implementing the role of a UA or proxy. SCTP transport between the UE and P-CSCF is not supported in the present document. Support of the SCTP transport is currently not described in 3GPP TS 33.203 [19].

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

When a security association is used to access the IM CN subsystem, the UE and the P-CSCF shall send and receive request and responses other than initial REGISTER requests on the protected ports as described in 3GPP TS 33.203 [19]. For UEs loaded with a ISIM or USIM, the security association shall always be used to access the IM CN subsystem as described in 3GPP TS 33.203 [19].

NOTE 2: The usage of NASS-bundled authentication, which provides for the user authentication without creation of a security association, still requires convergence with equivalent 3GPP documents, along with ensuring interoperability and coexistence with other security mechanisms. This will be addressed in a future version of this document, and may introduce some revision of the procedures.

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

5 Application usage of SIP

5.1.1.1A Parameters contained in the ISIM

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

The ISIM application shall always be used for IMS authentication, if it is present, as described in 3GPP TS 33.203 [19].

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

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

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;

in accordance with the procedures in clause C.2.

The temporary public user identity is only used in REGISTER requests, i.e. initial registration, re-registration, UE-initiated deregistration. The UE shall not reveal to the user the temporary public user identity if the temporary public user identity is barred. The temporary public user identity is not barred if received by the UE in the P-Associated-URI header.

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

5.1.1.1B Parameters provisioned to a UE without ISIM or USIM

In case the UE contains neither a ISIM application nor a USIM, the parameters used by the UE to initiate the registration to the IM CN subsystem and for authentication shall be preconfigured in accordance with clause C.4.

5.1.1.2 Initial registration (with security association setup)

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

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].

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

   - the username field, 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) 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) containing the IP address of the UE in the hostport parameter or FQDN. If the UE supports GRUU (see table A.4, item A.4/53), it shall include a +sip.instance parameter containing the instance ID. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2), and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS communication services and IMS applications it intends to use in a sip.app-subtype feature tag according to draft-rosenberg-sip-app-media-tag [120] and RFC 3840 [62]. 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) a Via header set to include the IP address or FQDN of the UE in the sent-by field. For the UDP, 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, while for the TCP, the response is received on the TCP connection on which the request was sent;

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 port values see 3GPP TS 33.203 [19].

f) an 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-CCF) 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 IPsec layer algorithms for integrity and confidentiality protection as defined in 3GPP TS 33.203 [19] and shall announce support for them according to the procedures defined in RFC 3329 [48];

i) the Supported header containing the option tag "path", and if GRUU is supported, the option tag "gruu"; and

j) if a security association exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header set as specified for the access network technology (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 as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header;

NOTE 4: The UE can utilize additional URIs contained in the P-Associated-URI header, e.g. for application purposes.

c) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header;

d) 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 standalone transactions;

e) 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; and

NOTE 5: If the UE receives Authentication-Info, it will proceed as described in RFC 3310 [49].

f) find the Contact header within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" parameter or a "temp-gruu" parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity that was registered.

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) release all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2;

b) initiate a new P-CSCF discovery procedure as described in subclause 9.2.1;

c) 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.

On receiving the 420 (Bad Extension) response with the Unsupported header containing the option tag "sec-agree" to the REGISTER request, the UE may send another REGISTER request without a security association based on the procedures described in 5.1.1.2A. The decision may depend on the UE's capability.

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.

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

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

a) select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1;

b) if no response has been received when attempting to contact all P-CSCFs known by the UE, the UE may get a new set of P-CSCF-addresses as described in subclause 9.2.1; and

c) perform the procedures for initial registration as described in subclause 5.1.1.2.

NOTE 6: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

After a maximum of 5 consecutive unsuccessful initial registration attempts, the UE shall not automatically attempt any further initial registration via the same network and the same P-CSCF, for an implementation dependant time of at least:

a) the amount of time indicated in the Retry-After header of the 4xx, 5xx, or 6xx response received in response to the most recent registration request, if that header was present; or

b) 30 minutes, if the header was not present and the initial registration was automatically performed as a consequence of a failed reregistration; or

c) 5 minutes, if the header was not present and the initial registration was not performed as a consequence of a failed reregistration.

These limits do not apply if the UE is power cycled.

5.1.1.2A Initial registration without security association setup

The UE can register a public user identity with its contact address at any time after it has acquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

The UE shall send 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].

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

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

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

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

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) containing the IP address of the UE in the hostport parameter or FQDN. If the UE supports GRUU (see table A.4, item A.4/53), it shall include a +sip.instance parameter containing the instance ID. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2), and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS communication services and IMS applications it intends to use in a sip.app-subtype feature tag according to draft-rosenberg-sip-app-media-tag [120] and RFC 3840 [62]; and

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field;

f) an 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 2: The registrar (S-CCF) 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 Supported header containing the option tag "path", and if GRUU is supported, the option tag "gruu"; and

i) if available to the UE (as defined in the access technology specific annexes for each access technology), the P-Access-Network-Info header set as specified for the access network technology (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 standalone transactions; and

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

f) find the Contact header within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" parameter or a "temp-gruu" parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity that was registered.

On receiving a 305 (Use Proxy) response to the initial REGISTER request, the UE shall:

a) release all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2;

b) initiate a new P-CSCF discovery procedure as described in subclause 9.2.1;

c) 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.

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

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

a) select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1;

b) if no response has been received when attempting to contact all P-CSCFs known by the UE, the UE may get a new set of P-CSCF-addresses as described in subclause 9.2.1; and

c) perform the procedures for initial registration as described in subclause 5.1.1.2A.

NOTE 4: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

After a maximum of 5 consecutive unsuccessful initial registration attempts, the UE shall not automatically attempt any further initial registration via the same network and the same P-CSCF, for an implementation dependant time of at least:

a) the amount of time indicated in the Retry-After header of the 4xx, 5xx, or 6xx response received in response to the most recent registration request, if that header was present; or

b) 30 minutes, if the header was not present and the initial registration was automatically performed as a consequence of a failed reregistration; or

c) 5 minutes, if the header was not present and the initial registration was not performed as a consequence of a failed reregistration.

These limits do not apply if the UE is power cycled.

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 Subscription to the registration-state event package

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the user's registrar (S-CCF) 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 initial 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

f) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header set as specified for the access network technology (see subclause 7.2A.4); and

g) a Contact header set to contain the same IP address or FQDN, and when a security association exists with the protected server port value as in the initial registration.

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. If a SUBSCRIBE request to refresh a subscription fails with a non-481 response, the UE shall still consider the original subscription valid for the duration of the most recently known "Expires" value according to RFC 3265 [28]. Otherwise, the UE shall consider the subscription invalid and start a new initial subscription according to RFC 3265 [28].

5.1.1.4 User-initiated re-registration and registration of an additional public user identity (with security association)

The UE can perform the reregistration of a previously registered public user identity with its contact address at any time after the initial registration has been completed. The UE shall perform the reregistration over the existing set of security associations that is associated with the related contact address.

The UE can perform registration of additional public user identities at any time after the initial registration has been completed. The UE shall perform the registration of additional public user identities over the existing set of security associations that is associated with the related contact address.

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

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 one is available.

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

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, and containing the instance ID of the UE in the +sip.instance parameter, if the UE supports GRUU (see table A.4, item A.4/53). The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2), and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS communication services and IMS applications it intends to use in a sip.app-subtype feature tag according to draft-rosenberg-sip-app-media-tag [120] and RFC 3840 [62];

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field and for the UDP the protected server port value bound to the security association, while for the TCP, the response is received on the TCP connection on which the request was sent;

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-CCF) 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 for security and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

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 if GRUU is supported, the option tag "gruu"; and

k) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header set as specified for the access network technology (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 Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions;

NOTE 4: The UE can utilize additional URIs contained in the P-Associated-URI header, e.g. for application purposes.

c) 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; and

NOTE 5: If the UE receives Authentication-Info, it will proceed as described in RFC 3310 [49].

d) find the Contact header within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" parameter or a "temp-gruu" parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity that was registered.

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 the 420 (Bad Extension) response with the Unsupported header containing the option tag “sec-agree” to the REGISTER request, the UE may send another REGISTER request without a security association based on the procedures described in 5.1.1.2A. The decision may depend on the UE's capability.

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

On receiving a 305 (Use Proxy) response to the REGISTER request, the UE shall:

a) release all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2;

b) initiate a new P-CSCF discovery procedure as described in subclause 9.2.1;

c) 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.

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

1) stop processing of all ongoing dialogs and transactions and silently discard them locally; and

2) after releasing all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2, the UE may:

   a) select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1;

   b) if no response has been received when attempting to contact all P-CSCFs known by the UE, the UE may get a new set of P-CSCF-addresses as described in subclause 9.2.1; and

   c) perform the procedures for initial registration as described in subclause 5.1.1.2.

NOTE 6: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

5.1.1.4A User-initiated re-registration and registration of an additional public user identity without security association

The UE can perform the reregistration of a previously registered public user identity with its contact address at any time after the initial registration has been completed.

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

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

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

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

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

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

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 containing the instance ID of the UE in the +sip.instance parameter, if the UE supports GRUU (see table A.4, item A.4/53). The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2), and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS communication services and IMS applications it intends to use in a sip.app-subtype feature tag according to draft-rosenberg-sip-app-media-tag [120] and RFC 3840 [62];

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field;

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 2: The registrar (S-CCF) 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 Supported header containing the option tag "path", and if GRUU is supported, the option tag "gruu"; and

i) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header set as specified for the access network technology (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;

NOTE 3: The UE can utilize additional URIs contained in the P-Associated-URI header, e.g. for application purposes.

b) 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 standalone transactions; and

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

c) find the Contact header within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" parameter or a "temp-gruu" parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity that was registered.

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

On receiving a 305 (Use Proxy) response to the REGISTER request, the UE shall:

a) release all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2;

b) initiate a new P-CSCF discovery procedure as described in subclause 9.2.1;

c) 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 5.1.1.2A.

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

1) stop processing of all ongoing dialogs and transactions and silently discard them locally; and

2) after releasing all IP-CAN bearers used for the transport of media according to the procedures in subclause 9.2.2, the UE may:

   a) select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1;

   b) if no response has been received when attempting to contact all P-CSCFs known by the UE, the UE may get a new set of P-CSCF-addresses as described in subclause 9.2.1; and

   c) perform the procedures for initial registration as described in subclause 5.1.1.2A.

NOTE 5: It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g. based on ICMP messages.

After a maximum of 5 consecutive initial registration attempts, the UE shall not automatically attempt any further initial registration for an implementation dependant time of at least 30 minutes.

5.1.1.5.1 General

Authentication is performed during initial registration as defined in subclause 5.1.1.2. A UE can be re-authenticated during subsequent re-registration s, deregistrations or registrations of additional public user identities as defined in subclause 5.1.1.4. 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 and CK (only if encryption enabled) 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 realm directive set to the value as received in the realm directive in the WWW Authenticate header, the private user identity and the authentication challenge response calculated by the UE using RES and other parameters, as described in RFC 3310 [49]. The UE shall also insert the Security-Client header 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 security association protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the security association 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 1: 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.

5.1.1.5.1A NASS-bundled authentication

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

5.1.1.5.2 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> sub-element that the UE registered to adjust the expiration time for that public user identity; and

2) start the re-authentication procedures at the appropriate time (as a result of the S-CCF procedure described in subclause 5.4.1.6) by initiating a reregistration as described in subclause 5.1.1.4, or subclause 5.1.1.4A if those procedures were performed for the initial authentication, if required.

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

5.1.1.5A Change of Ipv6 address due to privacy

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

If the UE receives an IPv6 prefix, the UE may change the interface identity of the IPv6 address as described in RFC 3041 [25A] due to privacy but this 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 subclause 5.1.1.6 or subclause 5.1.1.6A as appropriate to the authentication mechanism in use;

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 subclause 5.1.1.2 or subclause 5.1.1.2A as appropriate to the authentication mechanism in use; and

   b) by performing a subscription to the reg event package as described in subclause 5.1.1.3; and

5) subscribe to other event packages it was subscribed to before the change of IPv6 address procedure started.

5.1.1.6 User-initiated deregistration (with security association)

The UE can deregister a public user identity that it has previously registered with its contact address at any time.

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

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

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 However:

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

then the UE shall not release this dialog.

On sending a REGISTER request, 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 deregistered;

c) a To header set to the SIP URI that contains the public user identity to be deregistered;

d) a 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, and containing the Instance ID of the UE in the +sip.instance parameter, if the UE supports GRUU (see table A.4, item A.4/53);

e) a Via header set to include 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) an 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 for integrity and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

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) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header set as specified for the access network technology (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 IM CN subsystem.

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 2: 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.

5.1.1.6A User-initiated deregistration without security association

The UE can deregister a public user identity that it has previously registered with its contact address at any time.

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

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. However:

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

- this dialog is the only remaining dialog used for subscription to reg event package;

then the UE shall not release this dialog.

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

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

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

b) a From header set to the SIP URI that contains the public user identity to be deregistered;

c) a To header set to the SIP URI that contains the public user identity to be deregistered;

d) a 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 containing the Instance ID of the UE in the +sip.instance parameter, if the UE supports GRUU (see table A.4, item A.4/53);

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field;

f) an 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; and

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header set as specified for the access network technology (see subclause 7.2A.4).

On receiving the 200 (OK) response to the REGISTER request, the UE shall remove all registration details relating to this public user identity.

If all public user identities are deregistered, 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).

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) which were registered by this UE with:

- the state attribute set to "terminated" and the event attribute within the <contact> element belonging to this UE set to "rejected" or "deactivated"; or

- the state attribute set to "active" and within the <contact> element belonging to this UE, the state attribute set to "terminated" and the associated 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. or subclause 5.1.1.2A. In case of a "rejected" event attribute, the UE shall release all dialogs related to those public user identities.

Upon receipt of a NOTIFY request, the UE shall delete the security associations (if present) towards the P-CSCF either:

- if all <registration> element(s) have their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header contains the value of "terminated"; or

- if each <registration> element that was registered by this UE has either the state attribute set to "terminated", or the state attribute set to "active" and the state attribute within the <contact> element belonging to this UE set to "terminated".

The UE shall delete these security associations (if present) towards the P-CSCF after the server transaction (as defined in RFC 3261 [26]) pertaining to the received 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 all the public user identities or contact addresses registered by this UE are deregistered and the security association is removed, the UE considers the subscription to the reg event package terminated since the NOTIFY request was received with Subscription-State header containing the value of "terminated".

5.1.2A.1 UE-originating case

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

If a security association exists, when the UE sends any request, the UE shall send the request to the protected port received during registration as described in subclause 5.1.1.5.1 with:

- ~~include~~including the protected server port in the Via header entry relating to the UE.

Otherwise if no security association exists, i.e. no port is provided for subsequent SIP messages by P-CSCF during registration, the UE shall send any request to the same port used for the initial registration as described in subclause 5.1.1.2A.

If a security association exists, the UE shall discard any SIP response that is not protected by the security association 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 (contained in the P-Asserted-Identity header) within the IM CN subsystem.

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

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

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

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

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" as specified in RFC 3261 [26].

NOTE 5: 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 shall determine the public user identity to be used for this request as follows:

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

If this is a request for a new dialog, and the request includes a Contact header, then the UE should populate the Contact header as follows:

1) if a public GRUU value (pub-gruu) has been saved associated with the public user identity to be used for this request, and the UE does not indicate privacy of the P-Asserted-Identity, then insert the public GRUU (pub-gruu) value in the Contact header as specified in draft-ietf-sip-gruu [93]; or
2) if a temporary GRUU value (temp-gruu) has been saved associated with the public user identity to be used for this request, and the UE does indicate privacy of the P-Asserted-Identity, then insert the temporary GRUU (temp-gruu) value in the Contact header as specified in draft-ietf-sip-gruu [93]; or
3) if the request is related to an IMS communication service that requires the use of an ICSI then shall include in a sip.app-subtype feature tag the ICSI value (coded as specified in subclause 7.2A.8.2), for the IMS communication service and may include the IARI value (coded as specified in subclause 7.2A.9.2), that is related to the request according to draft-rosenberg-sip-app-media-tag [120] and RFC 3841 [56B]. The UE may also include other ICSI values that the UE is prepared to use for the communication and other IARI values for the IMS application that is related to the IMS communication service; or

4) if the request is related to an IMS application that is supported by the UE when the use of an ICSI is not needed, then may include the IARI value (coded as specified in subclause 7.2A.9.2), that is related to the to the IMS application, according to draft-rosenberg-sip-app-media-tag [120] and RFC 3841 [56B].

If this is a request within an existing dialog, and the request includes a Contact header, and the Contact address previously used in the dialog was a GRUU, then the UE should insert the previously used GRUU value in the Contact header as specified in draft-ietf-sip-gruu [93].

If the UE did not insert a GRUU in the Contact header, then the UE shall include the protected server port in the address in the Contact header.

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

1) shall include the ICSI value (coded as specified in subclause 7.2A.8.2), for the IMS communication service that is related to the request in a P-Preferred-Service header field according to draft-drage-sipping-service-identification [121];

2) may include an Accept-Contact header field containing an ICSI value (coded as specified in subclause 7.2A.8.2) or an IARI value (coded as specified in subclause 7.2A.9.2) that is related to the request in a sip.app-subtype feature tag according to draft-rosenberg-sip-app-media-tag [120] and RFC 3841 [56B] if the ICSI or IARI for the IMS communication service is known.

Editor's note: It is FFS whether the UE shall always include an ICSI value in an Accept-Contact header field. This also may need some clarifications to the stage 2 text to fully align.

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

NOTE 6: RFC 3841 [56B] allows multiple Accept-Contact header fields along with multiple Reject-Contact header fields in a SIP request, and within those header fields, expressions that include one or more logical operations based on combinations of feature tags. Which registered UE will be contacted depends on the Accept-Contact header field and Reject-Contact header field combinations included that evaluate to a logical expression and the relative qvalues of the registered contacts for the targeted registered public user identity. There is therefore no guarantee that when multiple Accept-Contact header fields or additional Reject-Contact header field(s) along with the Accept-Contact header field containing the ICSI value or IARI value are included in a request that the request will be routed to a contact that registered the same ICSI value or IARI value. Charging and accounting is based upon the contents of the P-Asserted-Service header field and the actual media related contents of the SIP request and not the Accept-Contact header field contents or the contact reached.

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

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

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

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

NOTE 8: During the dialog, the points of attachment to the IP-CAN of the UE may change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header 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 server 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 re-registration.

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

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause 5.1.1.4, or subclause 5.1.1.4A as appropriate to the authentication mechanism in use.

NOTE 9: It is an implementation option whether these actions are also triggered by other means.

The UE may use non-international formats of E.164 addresses, including geo-local numbers and home-local numbers, in the Request-URI.

NOTE 10: The way how the UE defines the default network for the numbers in a non-international format is implementation specific.

NOTE 11: The way how the UE process the dial-string and handles special characters (e.g. pause) in order to produce a conformant SIP URI or tel URI according to RFC 3966 [22] is implementation specific.

NOTE 12: Home operator's local policy can define a prefix string(s) to enable subscribers to differentiate dialling a geo-local number and/or a home-local number.

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

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

- if access technology information available to the UE (i.e., the UE can insert P-Access-Network-Info header into the request), include the access technology information in the "phone-context" parameter according to RFC 3966 [22] as defined in subclause 7.2A.10; and

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

NOTE 13: The "phone-context" parameter value can be entered by the subscriber, or can be inserted by the UE, based on implementation.

5.1.2A.2 UE-terminating case

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

If a security association exists, 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.

If an initial request contains an Accept-Contact header field containing a sip.app-subtype feature tag the UE should invoke the IMS application that is the best match for the ICSI value and if included IARI value contained in the sip.app-subtype feature tag. The UE can receive multiple Accept-Contact header fields containing sip.app-subtype feature tags. In this case it is up to the implementation which of the multiple ICSI values or IARI values it takes action on.

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 UE-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.

NOTE 2: A number of headers can reveal information about the identity of the user. Where, privacy is required, implementers should also give consideration to other headers that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of headers.

If the response includes a Contact header, and the response is sent within an existing dialog, and the Contact address previously used in the dialog was a GRUU, then the UE should insert the previously used GRUU value in the Contact header as specified in draft-ietf-sip-gruu [93].

If the response includes a Contact header, and the response is not sent within an existing dialog, then the UE should populate the Contact header as follows:

1) if a public GRUU value (pub-gruu) has been saved associated with the public user identity from the P-Called-Party-ID header, and the UE does not indicate privacy of the P-Asserted-Identity, then insert the public GRUU (pub-gruu) value in the Contact header as specified in draft-ietf-sip-gruu [93]; or

2) if a temporary GRUU value (temp-gruu) has been saved associated with the public user identity from the P-Called-Party-ID header, and the UE does indicate privacy of the P-Asserted-Identity, then the UE should insert the temporary GRUU (temp-gruu) value in the Contact header as specified in draft-ietf-sip-gruu [93]; or

3) if the request is related to an IMS communication service that requires the use of an ICSI then shall include in a sip.app-subtype feature tag the ICSI value (coded as specified in subclause 7.2A.8.2), for the IMS communication service and may include the IARI value for the IMS application, (coded as specified in subclause 7.2A.9.2), that is related to the request according to draft-rosenberg-sip-app-media-tag [120] and RFC 3841 [56B]. The UE may also include other ICSI values and other IARI values that is related to the IMS communication service that the UE is prepared to use; or

4) if the request is related to an IMS application that is supported by the UE when the use of an ICSI is not needed, then may include the IARI value (coded as specified in subclause 7.2A.9.2), that is related to the to the IMS application, according to draft-rosenberg-sip-app-media-tag [120] and RFC 3841 [56B].

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

If the UE did not insert a GRUU in the Contact header, then the UE shall include the protected server port in the address in the Contact header.

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

5.2.1 General

Subclause 5.2.2 through subclause 5.2.9 define P-CSCF procedures for SIP that do not relate to emergency. All SIP requests are first screened according to the procedures of subclause 5.2.10 to see if they do relate to an emergency.

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;

- 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-CCF, IBCF, or I-CSCF. Instead, the P-CSCF discovers charging function addresses by other means not specified in this document.

- remove any P-Access-Network-Info header if such header contains a "network-provided" parameter; and

- if the P-CSCF has access to a NASS supporting the UE, and the request is not an ACK request or CANCEL request or CANCEL response, add a P-Access-Network-Info header field that contains the "network-provided" parameter, and include other parameters in the P-Access-Network-Info header in accordance with the information received from the NASS.

NOTE 2A: Addition of the P-Access-Network-Info header by proxies, and repetition of the P-Access-Network-Info header within the same request or response, requires an update to RFC 3455 before such usage is valid.

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

NOTE 3: When a security association was set up at registration, the P-CSCF will integrity protect all SIP messages sent to the UE outside of the registration and authentication procedures by using ~~a~~the security association. When a security association was set up at registration, the P-CSCF will discard any SIP message that is not protected by using ~~a~~the security association and is received outside of the registration and authentication procedures. The integrity and confidentiality protection and checking requirements on the P-CSCF within the registration and authentication procedures are defined in subclause 5.2.2.

For each registration, the P-CSCF determines the type of access security to apply:

- if the initial REGISTER contains the Security-Client header field, the P-CSCF shall behave as specified in subclause 5.2.2;

- otherwise, the P-CSCF shall behave as specified in subclause 5.2.2A.

With the exception of 305 (Use Proxy) responses, the P-CSCF shall not recurse on 3xx responses.

~~NOTE 4: If the P-CSCF is connected to a PDF the requirements for this interconnection is specified in the Release 6 version of this specification.~~

When the P-CSCF receives a SIP request or SIP response containing the P-Early-Media header, the P-CSCF may add, remove, or modify, the header depending on whether media will be allowed to traverse to/from the UE at the point when the header is received.

NOTE ~~5~~4: The P-CSCF can use the header for the gate control procedures, as described in 3GPP TS 29.214 [13D].

In case a device performing address and/or port number conversions is provided by a NA(P)T or NA(P)T-PT controlled by the P-CSCF, the P-CSCF may need to modify the SIP contents according to the procedures described in annex F. In case a device performing address and/or port number conversions is provided by a NA(P)T or NA(P)T-PT not controlled by the P-CSCF, the P-CSCF may need to modify the SIP contents according to the procedures described in annex K if both a reg-id and instance ID parameter are present in the received contact header as described in draft-ieft-outbound [92].

5.2.2 Registration (with security association set-up)

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 only 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-CCF towards the P-CSCF) are expected to be treated as for the UE-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;

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 32.260 [17] and a type 1 orig-ioi parameter. The P-CSCF shall set the type 1 orig-ioi parameter to a value that identifies the sending network of the request. The P-CSCF shall not include the type 1 term-ioi parameter;

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 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 and with no authentication challenge response (i.e. no RES parameter), otherwise insert the parameter with the value "no";

5) in case the REGISTER request was received without protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. If the header is not present, then the P-CSCF shall return a suitable 4xx response;

6) in case the REGISTER request was received 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;

   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;

      - 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-CCF; and

   c) check if the private user identity conveyed in the Authorization header of the protected REGISTER request is the same as the private user identity which was previously challenged 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;

8) if the p-CSCF is located in the visited network, and local policy requires the application of IBCF capabilities in the visited network towards the home network, forward the request to an IBCF in the visited network

   If the selected exit point:

   - does not respond to the REGISTER request and its retransmissions by the P-CSCF; or

   - sends back a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request;

   the p-CSCF shall select a new exit point and forward the original REGISTER request.

NOTE 1: The list of the exit points can be either obtained as specified in RFC 3263 [27A] or provisioned in the P-CSCF.

   If the P-CSCF fails to forward the REGISTER request to any exit point, the P-CSCF shall send back a 504 (Server Time-Out) response to the user, in accordance with the procedures in RFC 3261 [26] unless local policy allows omitting the exit point; and

NOTE 2: If the P-CSCF forwards the request to an IBCF in the visited network, the IBCF can determine the entry point of the home network, using the same mechanisms as described in note 1 above. In that case the P-CSCF does not need to determine the entry point of the home network.

9) determine the entry point of the home network and forward the request to that entry point.

If the selected entry point:

- does not respond to the REGISTER request and its retransmissions by the P-CSCF; or
- sends back a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request;

the P-CSCF shall select a new entry point and forward the original REGISTER request.

NOTE 3: The list of the entry points can be either obtained as specified in RFC 3263 [27A] or provisioned in the P-CSCF.

If the P-CSCF fails to forward the REGISTER request to any entry point, the P-CSCF shall send back a 504 (Server Time-Out) response to the user, in accordance with the procedures in RFC 3261 [26].

When the P-CSCF receives a 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 IPsec layer algorithms for integrity and confidentiality protection as defined in 3GPP TS 33.203 [19] and shall announce support for them according to the procedures defined in RFC 3329 [48];

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 4: The challenge in the 401 (Unauthorized) response sent back by the S-CCF 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-CCF 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, including any associated display names, and associate them to the registered public user identity, i.e. the registered public user identity and its associated set of implicitly registered public user identities;

4) store the default public user identity, including its associated display name, if provided, 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 5: There can be more than one default public user identity stored in the P-CSCF, as the result of the multiple registrations of public user identities.

5) store the values received in the P-Charging-Function-Addresses header;

6) if a term-ioi parameter is received in the P-Charging-Vector header, store the value of the received term-ioi parameter;

NOTE 6: Any received term-ioi parameter will be a type 1 term-ioi. The type 1 term-ioi identifies the home network of the registered user.

7) 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;

8) if a temporary set of security associations exists, change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and

9) 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 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 7: 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 8: When receiving a SIP message (including REGISTER requests) from the UE over a set of security associations that is different from the newly established set of security associations, the P-CSCF will not take any action on any set of security associations.

When the SIP level lifetime of an old set of security associations is about to expire, i.e. their SIP level lifetime is shorter than 64*T1 and a newly established set of security associations has not been taken into use, the P-CSCF shall use the newly established set of security associations for further messages towards the UE as appropriate (see note 5).

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) response 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 9: 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 re-authentication 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

5.2.2A Registration without security association set-up

The P-CSCF shall be prepared to receive 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-CCF towards the P-CSCF) are expected to be treated as for the UE-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;

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 32.260 [17] and a type 1 orig-ioi parameter. The P-CSCF shall set the type 1 orig-ioi parameter to a value that identifies the sending network of the request. The P-CSCF shall not include the type 1 term-ioi parameter;

4) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network;

5) if the P-CSCF is located in the visited network, and local policy requires the application of IBCF capabilities in the visited network towards the home network, forward the request to an IBCF in the visited network

If the selected exit point:

- does not respond to the REGISTER request and its retransmissions by the P-CSCF; or

- sends back a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request;

the P-CSCF shall select a new exit point and forward the original REGISTER request.

NOTE 1: The list of the exit points can be either obtained as specified in RFC 3263 [27A] or provisioned in the P-CSCF.

If the P-CSCF fails to forward the REGISTER request to any exit point, the P-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] unless local policy allows omitting the exit point; and

NOTE 2: If the P-CSCF forwards the request to an IBCF in the visited network, the IBCF can determine the entry point of the home network, using the same mechanisms as described in note 1 above. In that case the P-CSCF does not need to determine the entry point of the home network.

6) determine the entry point of the home network and forward the request to that entry point.

If the selected entry point:

- does not respond to the REGISTER request and its retransmissions by the P-CSCF; or

- sends back a 3xx response or 480 (Temporarily Unavailable) response to a REGISTER request;

the P-CSCF shall select a new entry point and forward the original REGISTER request.

NOTE 3: The list of the entry points can be either obtained as specified in RFC 3263 [27A] or provisioned in the P-CSCF.

If the P-CSCF fails to forward the REGISTER request to any entry point, the P-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].

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 an association between the IP source address and port of the initial REGISTER request and the public user identities found in the P-Associated-URI header value and associate them to the public user identity under registration;

4) store an association between the IP source address and port of the initial REGISTER request the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 4: There can be more than one default public user identity stored in the P-CSCF, as the result of the multiple registrations of public user identities.

5) store the values received in the P-Charging-Function-Addresses header;

6) if a term-ioi parameter is received in the P-Charging-Vector header, store the value of the received term-ioi parameter;

NOTE 5: Any received term-ioi parameter will be a type 1 term-ioi. The type 1 term-ioi identifies the home network of the registered user.

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 or subclause 5.2.2A) sent by this UE, 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 belonging to this UE and all related stored information; and

2) check if the UE has left any other registered public user identity. When all of the public user identities that were registered by this UE are deregistered, the P-CSCF shall delete the security associations (if present) towards the UE, 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 (if present) 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 of the UE, as described in subclause 5.2.3, including one or more <registration> element(s) which were registered by the UE with either:

- the state attribute set to "terminated"; or

- the state attribute set to "active" and the state attribute within the <contact> sub-element belonging to this UE set to "terminated", and the event attribute within the <contact> sub-element belonging to this UE set to "rejected" or "deactivated";

the P-CSCF shall remove all stored information for these public user identities for this UE and remove these public user identities from the list of the public user identities that are registered for the user.

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" or when all public user identities of the UE have been deregistered, the P-CSCF shall shorten any existing security associations towards the UE.

NOTE 1: The security association between the P-CSCF and the UE is shortened to a value that will allow the NOTIFY request containing the deregistration event to reach the UE.

NOTE 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-CCF with an Expires header containing a value of zero).

5.2.6.2 Determination of UE-originated or UE-terminated case

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

- perform the procedures for the UE-terminating case as described in subclause 5.2.6.4 if the request makes use of the information for UE-terminating calls, which was added to the Path header entry of the P-CSCF during registration (see subclause 5.2.2 or subclause 5.2.2A), 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 UE-originating case as described in subclause 5.2.6.3 if this information is not used by the request.

5.2.6.3 Requests initiated by the UE

When the P-CSCF receives from the UE 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.

NOTE 1: If no security association was set-up during registration, the P-CSCF identifies the initiator of the request by matching the IP source address and port of the request with the IP source address entries stored during the registration for which it holds the list of registered public user identities.

When the P-CSCF receives from the UE an initial request for a dialog or a request for a standalone transaction, and the request contains a 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 than one default public user identity available, the P-CSCF shall randomly select one of them.

NOTE 2: If no security association was set-up during registration, the P-CSCF identifies the initiator of the request by matching the IP source address and port of the request with the IP source address entries stored during the registration for which it holds one or more default public user identities.

NOTE 3~~1~~: The contents of the From header do not form any part of this decision process.

NOTE 4~~2~~: The display-name portion of the P-Preferred-Identity header and the registered public user identities is not included in the comparison to determine a match.

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 re-registration) 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-CSCF shall either:

   a) return a 400 (Bad Request) response; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or

   b) replace the preloaded Route header 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) if the P-CSCF is located in the visited network, and local policy requires IBCF capabilities in the visited network towards the home network, then the P-CSCF shall select an IBCF in the visited network and add the URI of the selected IBCF to the topmost Route header;

NOTE 5~~3~~: It is implementation dependent as to how the P-CSCF obtains the address of the IBCF exit point.

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 in accordance with the procedures of RFC3261 [26], and either:

   a) the P-CSCF FQDN that resolves to the IP address; or

   b) the P-CSCF IP address;

4) when adding its own SIP URI to the top of the Record-Route header, build the P-CSCF SIP URI in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:

   a) the P-CSCF FQDN that resolves to the IP address; or

   b) the P-CSCF IP address;

5) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value including the display name if previously stored during registration representing the initiator of the request;

6) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]; and

7) 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 any 1xx or 2xx response to the above request, the P-CSCF shall:

1) store the values received in the P-Charging-Function-Addresses header;

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) if a security association exists, in the response rewrite its own Record Route entry to its own SIP URI that contains the protected server port number of the security association 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 46: 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; or

   b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;

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) when adding its own SIP URI to the Record-Route header, build the P-CSCF SIP URI in a format that contains the port number of the P-CSCF where it awaits subsequent requests from the called party, and either:

   a) the P-CSCF FQDN that resolves to the IP address; or

   b) the P-CSCF IP address; 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 ~~5~~7: 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) if a security association exists, rewrite the ~~the~~ address and port number of its own Record Route entry to the same value as for the response to the initial request for the dialog; and

2) replace the saved Contact header value received in the response such that the P-CSCF is able to release the session if needed;

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

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 re-registration) 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-CSCF shall either:

   a) return a 400 (Bad Request) response; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

   b) replace the preloaded Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response;

2) if the P-CSCF is located in the visited network, and local policy requires IBCF capabilities in the visited network towards the home network, then the P-CSCF shall select an IBCF in the visited network and add the URI of the selected IBCF to the topmost Route header;

NOTE ~~6~~8: It is implementation dependent as to how the P-CSCF obtains the address of the IBCF exit point.

3) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value, including the display name if previously stored during registration, representing the initiator of the request; and

4) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [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; or

   b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;

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) for dialogs that are not INVITE dialogs, add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]; and

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:

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) 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;

2) if the P-CSCF is located in the visited network, and local policy requires IBCF capabilities in the visited network towards the home network, then the P-CSCF shall select an IBCF in the visited network and add the URI of the selected IBCF to the topmost Route header; and

NOTE ~~7~~9: It is implementation dependent as to how the P-CSCF obtains the address of the IBCF exit point.

3) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value, including the display name if previously stored during registration, 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) convert the list of Record-Route header values into a list of Route header values and save this list of Route headers;

2) 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;

3) when adding its own SIP URI to the top of the list of Record-Route headers and save the list, build the P-CSCF SIP URI in a format that contains if a security association exists 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;

4) when adding its own address to the top of the received list of Via header and save the list, build the P-CSCF Via header entry in a format that contains, if a security association exists 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].

5) remove and store the values received in the P-Charging-Function-Addresses header;

6) remove and store the icid parameter received in the P-Charging-Vector header; and

7) 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 any 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 saved public user identity from the P-Called-Party-ID header that was received in the request, plus the display name if previously stored during registration, representing the initiator of the response;

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, if a security association exists add the port number of its own Record-Route entry with its own SIP URI with the port number where it awaits subsequent requests from the calling party and either:

      - the P-CSCF FQDN that resolves to its IP address; or

      - the P-CSCF IP address; and

      - remove the comp parameter if present.

      If the verification is successful, the P-CSCF shall, if a security association exists, rewrite its own Record-Route entry to its SIP URI in a format that contains the port number where it awaits subsequent requests from the calling party and either:

   - the P-CSCF FQDN that resolves to its IP address; or

   - the P-CSCF IP address; and

- remove the comp parameter if present;

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) 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 if a security association exists, 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 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].

2) when adding its own SIP URI to the top of the list of Record-Route headers and save the list, build the P-CSCF SIP URI in a format that contains if a security association exists, 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

3) for INVITE dialogs, replace the saved Contact and Cseq header field values received in the request such that the P-CSCF is able to release the session if needed;

NOTE 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) if a security association exists, rewrite the address and port number of its own Record-Route entry to the same value as for the response to the initial request for the dialog and remove the comp parameter; and

3) replace the saved Contact header field value received in the response such that the P-CSCF is able to release the session if needed;

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) if a security association exists, rewrite the IP address and the port number of its own Record-Route entry to the IP address and the port number where it awaits subsequent requests from the calling party and remove the comp parameter if present;

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 if a security association exists, 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) store the values received in the P-Charging-Function-Addresses header;

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

4) 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 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 saved public user identity from the P-Called-Party-ID header of the request, plus the display name if previously stored during registration, representing the initiator of the response;

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 if a security association exists, 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 5: 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].

5.2.7.2 UE-originating case

When the P-CSCF receives from the UE an INVITE request, the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, it shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

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

If a PCRF exists for the user for which a request is received, the P-CSCF shall also include the access-network-charging-info parameter (if received via the PCRF over the Rx or Gx interfaces) in the P-Charging-Vector header in the first request originated by the UE that traverses the P-CSCF, as soon as the charging information is available in the P-CSCF, e.g., after the local resource reservation is complete. Typically, this first request is an UPDATE request if the remote UA supports the "integration of resource management in SIP" extension or a re-INVITE request if the remote UA does not support the "integration of resource management in SIP" extension. See subclause 5.2.7.4 for further information on the access network charging information.

5.2.7.3 UE-terminating case

When the P-CSCF receives an INVITE request destined for the UE the P-CSCF may require the periodic refreshment of the session to avoid hung states in the P-CSCF. If the P-CSCF requires the session to be refreshed, it shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it in order to make it work.

When the P-CSCF receives an initial INVITE request destined for the UE, it will contain the Contact 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 request to the URI found in the Request-URI, the P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

If a PCRF exists for the user for which a request or response is received, the P-CSCF shall also include the access-network-charging-info parameter (if received via the PCRF, over the Gr or Gx interfaces) in the P-Charging-Vector header in the first request or response originated by the UE that traverses the P-CSCF, as soon as the charging information is available in the P-CSCF e.g., after the local resource reservation is complete. Typically, this first response is a 180 (Ringing) or 200 (OK) response if the remote UA supports the "integration of resource management in SIP" extension, or a re-INVITE request if the remote UA does not support the "integration of resource management in SIP" extension. See subclause 5.2.7.4 for further information on the access network charging information.

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 multimedia session currently being established (e.g. abort session request from PCRF), or of an indication that bearer resources are no longer available for a multimedia session currently being established (e.g. abort session request received from SPDF over the Gq' interface), the P-CSCF shall cancel that dialog by applying the following steps:

1) if the P-CSCF serves the calling user of the session, send out a CANCEL request to cancel the INVITE request towards the terminating UE that includes a Reason header containing a 503 (Service Unavailable) status code according to the procedures described in RFC 3261 [26] and RFC 3326 [34A]; and

2) if the P-CSCF serves the called user of the session, send out a 503 (Service Unavailable) response to the received INVITE request.

Upon receipt of an indication that QoS resources are no longer available for a multimedia session currently being established (e.g. abort session request from PCRF), or of an indication that bearer resources are no longer available for a multimedia session currently being established (e.g. abort session request received from SPDF over the Gq' interface), the P-CSCF shall cancel that dialog by responding to the original INVITE request with a 503 (Service Unavailable) response, and by sending out a CANCEL request to the INVITE request towards the terminating UE that includes a Reason header containing a 503 (Service Unavailable) status code according to the procedures described in RFC 3261 [26] and RFC 3326 [34A].

5.2.8.1.2 Release of an existing session

Upon receipt of an indication that the radio/bearer interface resources are no longer available for a session (e.g. abort session request PCRF), or of an indication that bearer resources are no longer available for a multimedia session currently being established (e.g. abort session request received from SPDF over the Gq' interface) or upon detecting that the SDP offer conveyed in a SIP response contained parameters which are not allowed according to the local policy (as specified in the subclause 6.2), the P-CSCF shall release the respective dialog by applying the following steps:

1) if the P-CSCF serves the calling user of the session 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;
   - a Reason header that contains:
     - a 503 (Service Unavailable) response code, if radio/bearer ~~interface~~ resources are no longer available; or

- a 488 (Not Acceptable Here) response code, if a SDP offer conveyed in a SIP response contained parameters which are not allowed according to the local policy; and

- further headers, based on local policy.

2) If the P-CSCF serves the called user of the 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;

   - a Reason header that contains:

     - a 503 (Service Unavailable) response code;, if radio/bearer ~~interface~~ resources are no longer available; or

     - a 488 (Not Acceptable Here) response code, if SDP payload contained parameters which are not allowed according to the local policy; and

   - further headers, based on local policy.

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.

5.2.8.1.4 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 Rx or Gx or Gq' interface that the session has been terminated.

5.2.8.3 Session expiration

If the P-CSCF requested the session to be refreshed periodically, and the P-CSCF got the indication that the session will be refreshed, when the session timer expires, the P-CSCF shall delete all the stored information related to the dialog.

NOTE: The P-CSCF will also indicate to the IP-CAN, via the Rx or Gx or Gq' interface, that the session has terminated.

5.2.10.1 General

If the P-CSCF belongs to a network where the registration is not required to obtain emergency service, the P-CSCF shall accept any unprotected request on the IP address and port advertised to the UE during the P-CSCF discovery procedure. The P-CSCF shall also accept any unprotected request on the same IP address and the default port as specified in RFC 3261 [26].

The P-CSCF can handle emergency session and other requests from both a registered user as well as an unregistered user. Certain networks only allow emergency session from registered users.

~~NOTE 1: If only emergency setup from registered users is allowed, a request from an unregistered user is ignored since it is received outside of the security association.~~

The P-CSCF shall not subscribe to the reg event package for any emergency public user identity.

The P-CSCF shall store a configurable list of local emergency service identifiers, i.e. emergency numbers and the emergency service URN, which are valid for 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 service identifiers.

NOTE ~~2~~1: The emergency service URN are common to all networks, although subtypes may either not necessarily be in use, or a different set of subtypes is in use. The above requirements do not apply to subtypes of the emergency service URN.

Access technology specific procedures are described in each access technology specific annex to determine whether the initial request for a dialog or standalone transaction or an unknown method is destined for a PSAP.

NOTE ~~3~~2: Depending on local operator policy, the P-CSCF has the capability to reject requests relating to specific methods in accordance with RFC 3261 [26], as an alternative to the functionality described above.

When the P-CSCF responds that the CS domain is to be used for emergency call 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 <alternative-service> element, set to the parameters of the alternative service:

b) a <type> child element, set to "emergency" to indicate that it was an emergency call; and

c) a <reason> child element, set to an operator configurable reason.

The P-CSCF can handle emergency session establishment within a non-emergency registration.

When the P-CSCF responds that an emergency registration is required 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 <alternative-service> element, set to the parameters of the alternative service;

b) a <type> child element, set to "emergency" to indicate that it was an emergency call; and

c) an <action> child element, set to "emergency-registration" to indicate that emergency registration is required; and

d) a <reason> child element, set to an operator configurable reason.

NOTE ~~4~~3: <action> element is used only in a context to indicate the UE that emergency registration is required in the present document. Therefore, this element is defined as optional and shall not be used in other purpose.

NOTE ~~5~~4: This response is only sent in case if the P-CSCF received an explicit indication from the UE that it is an emergency session, i.e. receive emergency service URN in the Request-URI.

For all SIP transactions identified as relating to an emergency, the P-CSCF shall give priority over other transactions. This allows special treatment (e.g. with respect to filtering, higher priority, routeing) of emergency sessions. The exact meaning of priority is not defined further in this document, but is left to national regulation and network configuration.

5.2.10.3 General treatment for all dialogs and standalone transactions excluding the REGISTER method after emergency registration

If the P-CSCF receives an initial request for a dialog, or a standalone transaction, or an unknown method, for a registered user ~~over the security association that was created during the emergency registration~~, the P-CSCF shall inspect the Request URI independent of values of possible entries in the received Route headers for known emergency service identifiers, i.e. emergency numbers and the emergency service URN from these configurable lists.

If the P-CSCF detects that the Request-URI of the initial request for a dialog, or a standalone transaction, or an unknown method does not match any one of the emergency service identifiers in any of these lists, the P-CSCF shall reject the request by returning a 403 (Forbidden) response to the UE.

If the P-CSCF detects that the Request-URI of the initial request for a dialog, or a standalone transaction, or an unknown method matches one of the emergency service identifiers in any of these lists, the P-CSCF shall:

1) include in the Request-URI an emergency service URN, i.e. with a service type of "sos" as specified in draft-ietf-ecrit-service-urn [69], if necessary, and execute the procedure described in step 3, 4, 5, and 6, in subclause 5.2.6.3 dealing with the procedure when the P-CSCF receives an initial request from the UE. The entry in the Request-URI that the P-CSCF includes may either be:

   - as received from the UE in the Request URI in accordance with draft-ietf-ecrit-service-urn [69]; or

   - as deduced from the Request-URI received from the UE.

2) if the request contains a Contact header field containing a GRUU the P-CSCF shall save the GRUU received in the Contact header field of the request and associate it with the UE IP address and UE ~~protected~~ server port, ~~for the security association on which the request was received~~ such that the P-CSCF is able to route target refresh request containing that GRUU in the Request-URI; and

In addition the P-CSCF shall execute the procedures as specified in subclause 5.2 with the following additions:

3) the P-CSCF shall:

   - if the registered emergency public user identity is included in the P-Preferred-Identity header, remove the P-Preferred-Identity header from the received request and insert a P-Asserted-Identity header that includes the emergency public user identity that was present in the P-Preferred-Identity header. Add a second P-Asserted identity header that contains the tel URI associated with the emergency public user identity. If the tel URI associated with the registered emergency public user identity is included in the P-Preferred-Identity header, check the validity of the tel URI, remove the P-Preferred-Identity header and insert a P-Asserted-Identity header that includes the tel URI that was present in the P-Preferred-Identity header. Add a second P-Asserted-Identity header that contains the emergency public user identity; and

   - select an E-CSCF and add the URI of the selected E-CSCF to the topmost Route header.

NOTE: It is implementation dependant as to how the P-CSCF obtains the list of E-CSCFs.

If the P-CSCF does not receive any response to the INVITE request (including its retransmissions); or receives a 3xx response or 480 (Temporarily Unavailable) response to an INVITE request, the P-CSCF shall select a new E-CSCF and forward the INVITE request.

When the P-CSCF receives a target refresh request for a dialog with the Request-URI containing a GRUU the P-CSCF shall:

- obtain the UE IP address and UE protected server port related to the GRUU contained in the Request-URI and rewrite the Request-URI with that UE IP address and UE protected server port; and

- perform the steps in subclause 5.2.6.4 for when the P-CSCF receives, destined for the UE, a target refresh request for a dialog.

5.4.1.1 Introduction

The S-CCF shall act as the SIP registrar for all UAs belonging to the IM CN subsystem and with public user identities.

Subclause 5.4.1.2 through subclause 5.4.1.7 define S-CCF procedures for SIP registration that do not relate to emergency. All registration requests are first screened according to the procedures of subclause 5.4.8.2 to see if they do relate to an emergency public user identity.

The S-CCF shall support the use of the Path and Service-Route header. The S-CCF shall 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 S-CCF shall not act as a redirect server for REGISTER requests.

The network operator defines minimum and maximum times for each registration. These values are provided within the S-CCF.

The procedures for notification concerning automatically registered public user identities of a user are described in subclause 5.4.2.1.2.

In case a device performing address and/or port number conversions is provided by a NA(P)T or NA(P)T-PT, the S-CCF may need to modify the SIP signalling according to the procedures described in annex K if both a reg-id and instance ID parameter are present in the received contact header as described in draft-ieft-outbound [92].

The S-CCF shall determine based on the contents of the REGISTER request whether procedure for IMS-AKA authentication are to be performed or not:

- if the REGISTER request contains an Authorization header field with the “integrity-protected” parameter, the S-CCF shall perform the initial registration procedures with IMS-AKA authentication described in subclause 5.4.1.2.1;

- otherwise (i.e. no Authorization header field is present, or Authorization header field is received without the "integrity-protected" parameter), the S-CCF shall perform the initial registration procedures as described in subclause 5.4.1.2A.

5.4.1.2 Initial registration and user-initiated reregistration with IMS-AKA authentication

5.4.1.2.1 Unprotected REGISTER

NOTE 1: Any REGISTER request sent unprotected with the "integrity-protected" parameter in the Authorization header set to "no" 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-CCF 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.

Upon receipt of a REGISTER request ~~without an "integrity-protected" parameter, or~~ with the "integrity-protected" parameter in the Authorization header set to "no", for a user identity linked to a private user identity that has a registered public user identity but with a new contact address, the S-CCF 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 there are public user identities belonging to this user that have been previously registered with an old contact address different from the one received in the REGISTER request and the previous registrations have not expired, the S-CCF shall perform the network initiated deregistration procedure for the previously registered public user identities and the associated old contact address as described in subclause 5.4.1.5.

NOTE 3: Contact related to emergency registration is not affected. S-CCF is not able deregister contact related to emergency registration and will not delete that.

When S-CCF receives a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "no" and a non-empty response directive, the S-CCF 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", which is not for an already registered public user identity linked to the same private user identity, the S-CCF 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 header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;

3) select an authentication vector for the user. If no authentication vector for this user is available, after the S-CCF has performed the Cx Multimedia Authentication procedure with the HSS, as described in 3GPP TS 29.228 [14], the S-CCF 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-CCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14] or use the value as received in the P-User-Database header in the REGISTER request as defined in RFC 4457 [82];

NOTE 4: The HSS address received in the response to SLF query or as a value of P-User-Database header can be used to address the HSS of the public user identity in further queries.

NOTE 5: At this point the S-CCF informs the HSS that the user currently registering will be served by the S-CCF by passing its SIP URI to the HSS. This will be used by the HSS to direct all subsequent incoming initial requests for a dialog or standalone transactions destined for this user to this S-CCF.

NOTE 6: When passing its SIP URI to the HSS, the S-CCF may include in its SIP URI the transport protocol and the port number where it wants to be contacted.

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-CCF 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 resynchronization. If a stored RAND already exists in the S-CCF, the S-CCF 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-CCF to the UE was deemed to be invalid by the UE, the S-CCF shall stop the timer reg-await-auth and proceed as described in the subclause 5.4.1.2.3.

5.4.1.2A Initial registration and user-initiated reregistration for non IMS-AKA authentication

Upon receipt of a REGISTER request without the "integrity-protected" parameter in the Authorization header or without an Authorization header, for a user identity linked to a private user identity that has a registered public user identity but with a new contact address, the S-CCF shall:

1) perform the procedure for receipt of a REGISTER request without the "integrity-protected" parameter in the Authorization header or without the Authorization header, for the received public user identity; and

2) if the authentication has been successful, and there are public user identities belonging to this user that have been previously registered with an old contact address different from the one received in the REGISTER request and if the previous registration have not expired, the S-CCF shall perform the network initiated deregistration procedure for the previously registered public user identities and the associated old contact address as described in subclause 5.4.1.5.

NOTE 1: Contact related to emergency registration is not affected. S-CCF is not able deregister contact related to emergency registration and will not delete that.

Upon receipt of a REGISTER request without the "integrity-protected" parameter in the Authorization header or without an Authorization header, which is not for an already registered public user identity linked to the same private user identity, the S-CCF shall:

1) identify the user by the public user identity as received in the To header of the REGISTER request and if the Authorization header is present, the private user identity as received in the Authorization header of the REGISTER request;

2) check if the P-Visited-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;

3) check whether one or more Line-Identifiers previously received over the Cx interface, and stored as a result of a Cx Multimedia Authentication procedure with the HSS, are available for the user. If not, the S-CCF shall perform the Cx Multimedia Authentication procedure with the HSS, as described in [14].

   Prior to performing Cx Multimedia Authentication procedure with the HSS, the S-CCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14] or use the value as received in the P-User-Database header in the REGISTER request as defined in RFC 4457 [82];

NOTE 2: The HSS address received in the response to SLF query or as a value of P-User-Database header can be used to address the HSS of the public user identity in further queries.

NOTE 3: At this point the S-CCF informs the HSS that the user currently registering will be served by the S-CCF by passing its SIP URI to the HSS. This will be used by the HSS to direct all subsequent incoming initial requests for a dialog or standalone transactions destined for this user to this S-CCF.

NOTE 4: When passing its SIP URI to the HSS, the S-CCF may include in its SIP URI the transport protocol and the port number where it wants to be contacted.

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

5) In the particular case where the S-CCF received via the Cx interface one or more Line-Identifiers, compare each of the ”dsl-location” parameter of the P-Access-Network-Info header field (if present and if it includes the “network-provided” parameter),

   -if one of these match, the user shall be considered authenticated and the S-CCF behave as described in step 5) to 13) of subclause 5.4.1.2.2;

   -otherwise i.e. if these do not match the S-CCF shall return a 403 (Forbidden) response to the REGISTER request; and

6) if no Line-Identifier is received over the Cx interface, send a 500 (Server Internal Error) response to the REGISTER request.

Upon receipt of a REGISTER request without the "integrity-protected" parameter in the Authorization header or without an Authorization header, for an already registered public user identity linked to the same private user identity, and for existing contact information, the S-CCF shall behave as described in step 6) to 13) of subclause 5.4.1.2.2.

5.4.1.2A.1 Abnormal cases

In the case that the expiration timer from the UE is too short to be accepted by the S-CCF, the S-CCF shall:

- reject the REGISTER request with a 423 (Interval Too Brief) response, containing a Min-Expires header with the minimum registration time the S-CCF 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-CCF may:

- abort sending third-party REGISTER requests; and

- initiate network-initiated deregistration procedure.

If the Filter Criteria does not contain instruction to the S-CCF regarding the failure of the contact to the AS, the S-CCF 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-CCF shall store:

- the entry in the Contact header with the highest "q"; or

- an entry decided by the S-CCF based on local policy;

and include it in the 200 (OK) response.

5.4.1.3 Authentication and reauthentication

Authentication and reauthentication is performed by the registration procedures as described in subclause 5.4.1.2 or 5.4.1.2A.

5.4.1.4 User-initiated deregistration

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

- check whether any of the following conditions apply. The S-CCF shall only proceed with the following steps if either one of the conditions is met;

  a) (case for using IMS-AKA authentication)the "integrity-protected" parameter in the Authorization header field set to "yes", indicating that the REGISTER request was received integrity protected; or

  b) (case for non IMS-AKA authentication)
  the "integrity-protected" parameter in the Authorization header field does not exist or without an Authorization header, and one or more Line-Identifiers previously received over the Cx interface, stored as a result of a Cx Multimedia Authentication procedure with the HSS, are available for the user;

~~The S-CCF shall only proceed with the following steps if the "integrity-protected" parameter is set to "yes";~~

- release all dialogs that includes this user, where the dialogs were initiated by this UE with the same public user identity found in the To header field that was received in the REGISTER request or with one of the implicitly registered public user identities by applying the steps listed in subclause 5.4.5.1.2. However:

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

  - this dialog is the only remaining dialog used for subscription to reg event package;

  then the S-CCF shall not release this dialog;

- if this public user identity was registered only by this UE, deregister the public user identity found in the To header field together with the implicitly registered public user identities. Otherwise, the S-CCF will only remove the contact address that was registered by this UE;

NOTE: If the UE sends a REGISTER request with the value "*" in the Contact header and the value zero in the Expires header, the S-CCF will only remove the contact address that was registered by this UE identified with its private user identity.

- 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 user identities, release each of these multimedia sessions 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-CCF 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~~contained the "integrity-protected" parameter ~~was~~ set to the value "no", the S-CCF 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 29.228 [14], for one or more public user identities, the S-CCF 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-CCF can request of the HSS to either be kept or cleared as the S-CCF allocated to this subscriber).

5.4.1.6 Network-initiated reauthentication

The S-CCF 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 or subclause 5.4.1.2A.

If the S-CCF is informed that a private user identity needs to be re-authenticated, the S-CCF 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-CCF 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-CCF is aware of the user owns:

   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE;

   b) set the aor attribute within each <registration> element to one public user identity;

   c) set the state attribute within each <registration> element to "active";

   d) set the state attribute within each <contact> element to "active";

   e) set the event attribute within each <contact> element that was registered by this UE to "shortened";

   f) set the expiry attribute within each <contact> element that was registered by this UE to an operator defined value; and

   g) set the <pub-gruu> and <temp-gruu> sub-elements within each <contact> element as specified in subclause 5.4.2.1.2; and

   NOTE 1: There might be more than one contact information available for one public user identity. The S-CCF will only modify the <contact> elements that were originally registered by this UE using its private user identity. The S-CCF will not modify the <contact> elements for the same public user identity, if registered by another UE using different private user identity.

4) set a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

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

NOTE 2: Network initiated re-authentication may occur due to internal processing within the S-CCF.

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

When generating the NOTIFY request, the S-CCF 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-CCF shall include a P-Access-Network-Info header and a P-Visited-Network-ID 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-CCF shall not include any P-Access-Network-Info header or P-Visited-Network-ID header. The S-CCF 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, 5.4.1.2A, 5.4.1.4 or 5.4.1.5 (as appropriate) was successful, the S-CCF 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-CCF'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 1: For the whole implicit registration set only one public user identity per service profile appears in the third-party REGISTER requests. Thus, based on third-party REGISTER requests only, the ASs will not have complete information on the registration state of each public user identity in the implicit registration set. The only way to have a complete and continuously updated information (even upon administrative change in subscriber's profile) is to subscribe to the reg event package.

d) the Contact header, which shall contain the S-CCF's SIP URI;

e) for initial registration and user-initiated reregistration (subclause 5.4.1.2 or subclause 5.4.1.2A), the Expires header, which shall contain the same value that the S-CCF returned in the 200 (OK) response for the REGISTER request received from the UE;

f) for user-initiated deregistration (subclause 5.4.1.4) and network-initiated deregistration (subclause 5.4.1.5), the Expires header, which shall contain the value zero;

g) for initial registration and user-initiated reregistration (subclause 5.4.1.2 or subclause 5.4.1.2A), 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). 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-CCF shall include it in the message body of the REGISTER request within the <service-info> XML element as described in subclause 7.6. For the messages including the IM CN subsystem XML body, the S-CCF 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, shall contain the same icid parameter that the S-CCF received in the original REGISTER request from the UE. The S-CCF shall insert a type 3 orig-ioi parameter in the P-Charging-Vector header. The type 3 orig-ioi parameter identifies the sending network of the request and add a type 3 orig-ioi parameter before the received orig-ioi parameter. The S-CCF shall set the type 3 orig-ioi parameter to a value that identifies the sending network of the request. The S-CCF shall not include the type 3 term-ioi parameter;

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-CCF home network; and

j) in case the original received REGISTER request contained a P-User-Database header and the AS belongs to the same operator as the S-CCF, optionally a P-User-Database header which shall contain the received value.

When the S-CCF receives any response to a third-party REGISTER request, the S-CCF shall store the value of the term-ioi parameter received in the P-Charging-Vector header, if present.

NOTE 2: Any received term-ioi parameter will be a type 3 term-ioi. The type 3 term-ioi identifies the service provider from which the response was sent.

When the S-CCF receives any response to third-party REGISTER, the S-CCF shall store the value of the type 3 term-ioi parameter received in the P-Charging-Vector header, if present. The type 3 term-ioi identifies the service provider from which the response was sent.

If the S-CCF fails to receive a SIP response or receives a 408 (Request Timeout) response or a 5xx response to a third-party REGISTER, the S-CCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION_CONTINUED" as specified in 3GPP TS 29.228 [14] or no default handling is indicated, no further action is needed; and

- if the default handling defined in the filter criteria indicates the value "SESSION_TERMINATED" as specified in 3GPP TS 29.228 [14], the S-CCF shall, for a currently registered public user identity, initiate the network-initiated deregistration as described in subclause 5.4.1.5.

5.4.3.2 Requests initiated by the served user

When the S-CCF receives from the served user or from a PSI an initial request for a dialog or a request for a standalone transaction, and the request is received either from a functional entity within the same trust domain or contains a valid original dialog identifier (see step 3) or the dialog identifier (From, To and Call-ID header fields) relates to an existing request processed by the S-CCF, then prior to forwarding the request, the S-CCF 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-CCF 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.

1A) if the Contact is a GRUU, but is not valid as defined in subclause 5.4.7A.4, then return a 4xx response as specified in draft-ietf-sip-gruu [93];

2) store the value of the orig-ioi parameter received in the P-Charging-Vector header if present, and remove it from any forwarded request;

NOTE 2: Any received orig-ioi parameter will be a type 3 orig-ioi. The type 3 orig-ioi identifies the service provider from which the request was sent (AS initiating a session on behalf of a user or a PSI);

3) check if an original dialog identifier that the S-CCF previously placed in a Route header is present in the topmost Route header of the incoming request. If not present, the S-CCF shall build an ordered list of initial filter criteria based on the public user identity in the P-Asserted-Identity header of the received request as described in 3GPP TS 23.218 [5]. If present, the request has been sent from an AS in response to a previously sent request, an ordered list of initial filter criteria already exists and it shall be kept unchanged even if the AS has changed the P-Asserted-Identity header;

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

4A) determine whether the contents of the request matches a subscribed service (i.e. SDP media capabilities, Content-Type header field) for each and any of the subscribed services for the served user. As an operator option, if the contents of the request do not match a subscribed service, the S-CCF may reject the request by generating a 403 (Forbidden) response. Otherwise, continue with the rest of the steps;

Editor's note: It is for further study whether the S-CCF shall authorise and police that the media types used by the served user is consistent with the ICSI value.

4B) if the request contains a P-Preferred-Service header field check whether the ICSI value contained in the P-Preferred-Service header field is part of the set of the subscribed services for the served user and if so then use that ICSI value as the value for the P-Asserted-Header field for the request and remove the P-Preferred-Service header field;

4C) if the request does not contain a P-Preferred-Service header field or the ICSI value contained in a P-Preferred-Service header field is not part of the set of the subscribed services for the served user then as an operator option, the S-CCF may reject the request by generating a 403 (Forbidden) response. Otherwise, continue with the rest of the steps;

4D) include a P-Asserted-Service header field in the request containing the ICSI value determined in step 4B and use as a header field in the initial request when matching initial filter criteria in step 5;

5) check whether the initial request matches the next unexecuted initial filter criteria from the ordered list of initial filter criteria, and if it does, the S-CCF 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;

   b) if the AS is located outside the trust domain then the S-CCF shall remove the P-Access-Network-Info header field and its values in the request and the access-network-charging-info parameter in the P-Charging-Vector header from the request that is forwarded to the AS; if the AS is located within the trust domain, then the S-CCF 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; and

   c) insert a type 3 orig-ioi parameter before the received orig-ioi parameters in the P-Charging-Vector header. The S-CCF shall set the type 3 orig-ioi parameter to a value that identifies the sending network of the request. The S-CCF shall not include the type 3 term-ioi parameter;

NOTE 3: Depending on the result of processing the filter criteria the S-CCF might contact one or more AS(s) before processing the outgoing Request URI.

NOTE 4: An AS can activate or deactivate its own filter criteria via the Sh interface. As the S-CCF checks initial filter criteria only on receipt of an initial request for a dialog, or a standalone transaction, a modified service profile will have no impact on transactions or dialogs already in progress and the modified profile will be effective only for new transactions and dialogs. If the S-CCF receives a modification of the iFC during their execution, then it should not update the stored initial Filter Criteria until the iFC related to the initial request have been completely executed.

6) if there 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-CCF 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-CCF creates a new icid, then it is responsible for maintaining the two icid values in the subsequent messaging;

7) in step 5, if the initial request did not match the next unexecuted initial filter criteria (i.e. the request is not forwarded to an AS), insert an orig-ioi parameter into the P-Charging-Vector header. The S-CCF shall set the orig-ioi parameter to a value that identifies the sending network. The S-CCF shall not include the type 2 term-ioi parameter;

8) 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-CCF home network, including towards AS;

9) if there is no original dialog identifier present in the topmost Route header of the incoming request and if the S-CCF has knowledge that the SIP URI contained in the received P-Asserted-Identity header is an alias SIP URI for a tel URI, add a second P-Asserted-Identity header containing this tel-URI, including the display name associated with the tel URI, if available. If the P-Asserted-Identity header contains only a tel URI, the S-CCF shall add a second P-Asserted-Identity header containing a SIP URI. The added SIP URI shall contain in the user part a "+" followed by the international public telecommunication number contained in tel URI, and user's home domain name in the hostport part. The added SIP URI shall contain the same value in the display name as contained in the tel URI. The S-CCF shall also add a user parameter equals "phone" to the SIP URI;

NOTE 5: The S-CCF recognizes that a given SIP URI is an alias SIP URI of a tel URI, since they have the same service profile and belong to the same set of implicitly registered public user identities. If tel URI is shared URI so is the alias SIP URI.

10) if the request is not forwarded to an AS and if the outgoing Request-URI is:

   - a SIP URI with the user part starting with a + and the user parameter equals "phone", and if configured per local operator policy, the S-CCF shall perform the procedure described here. Local policy can dictate whether this procedure is performed for all domains of the SIP URI, only if the domain belongs to the home network, or not at all. If local policy indicates that the procedure is to be performed, then the S-CCF shall translate the international public telecommunications number contained in the user part of the SIP URI (see RFC 3966 [22]) to a globally routeable SIP URI using either an ENUM/DNS translation mechanism with the format specified in RFC 3761 [24], or any other available database.

Database aspects of ENUM are outside the scope of the present document. An S-CCF that implements the additional routeing functionality described in annex I may forward the request without attempting translation. If a translation is in fact performed and it succeeds, the S-CCF shall update the Request-URI with the globally routeable SIP URI returned by ENUM/DNS. 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-CCF may send an appropriate SIP response to the originator. When forwarding the request to a BGCF or any other appropriate entity, the S-CCF shall leave the original Request-URI containing the SIP URI with user parameter equals phone unmodified. If the request is forwarded, the S-CCF shall remove the access-network-charging-info parameter from the P-Charging-Vector header prior to forwarding the message;

- a tel URI in the international format, the S-CCF shall translate the E.164 address (see RFC 3966 [22]) to a globally routeable SIP URI using either an ENUM/DNS translation mechanism with the format specified in RFC 3761[24] , or any other available database. Databases aspects of ENUM are outside the scope of the present document. An S-CCF that implements the additional routeing functionality described in annex I may forward the request without attempting translation. If this translation is in fact performed and it succeeds, the S-CCF shall update the Request-URI with the globally routeable SIP URI returned by ENUM/DNS. 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-CCF may send an appropriate SIP response to the originator. When forwarding the request to a BGCF or any other appropriate entity, the S-CCF shall leave the original Request-URI containing the tel URI unmodified. If the request is forwarded, the S-CCF shall remove the access-network-charging-info parameter from the P-Charging-Vector header prior to forwarding the message;

- a tel URI in non-international format (i.e. the local service number analysis and handling is either failed in the appropriate AS or the request has not been forwarded to AS for local service number analysis and handling at all), either forward the request to a BGCF or any other appropriate entity (e.g. a MRFC to play an announcement) in the originator's home network or send an appropriate SIP response to the originator; and

- a pres URI or an im URI, the S-CCF shall forward the request as specified in RFC 3861 [63]. In this case, the S-CCF shall not modify the received Request-URI;

11) 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. If the destination requires interconnect functionalities (e.g. the destination address is of an IP address type other than the IP address type used in the IM CN subsystem), the S-CCF shall forward the request the request shall be forwarded to the destination address via an IBCF in the same network;

12) if network hiding is needed due to local policy, put the address of the IBCF to the topmost route header;

13) in case of an initial request for a dialog:

   a) determine the need for GRUU processing. GRUU processing is required if:

      - an original dialog identifier that the S-CCF previously placed in a Route header is not present in the topmost Route header of the incoming request (this means the request is not returning after having been sent to an AS), and

      - the contact address contains a valid GRUU as specified in subclause 5.4.7A.4.

   b) if GRUU processing is not required and the initial request originated from a served user, then determine the need to record-route for other reasons:

      - if the request is routed to an AS which is part of the trust domain, the S-CCF can decide whether to record-route or not. The decision is configured in the S-CCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CCF shall create a Record-Route header containing its own SIP URI; or

      - if the request is routed elsewhere, create a Record-Route header containing its own SIP URI;

NOTE 6: For requests originated from a PSI the S-CCF can decide whether to record-route or not based on operator policy.

c) if GRUU processing is required, the S-CCF shall create a Record-Route header containing its own SIP URI;

d) if GRUU processing is required, the S-CCF shall save an indication that GRUU-routeing is to be performed for in-dialog requests that reach the S-CCF because of the Record-route header added in step c);

NOTE 7: The manner of representing the GRUU-routeing indication is a private matter for the S-CCF. The indication is used during termination processing of in-dialog requests to cause the S-CCF to replace a Request-URI containing a GRUU with the corresponding registered contact address. It can be saved using values in the Record-Route header, or in dialog state.

14) based on the destination user (Request-URI), 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;

15) route the request based on SIP routeing procedures; and

16) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CCF is able to release the session if needed.

When the S-CCF receives, an initial request for a dialog or a request for a standalone transaction, from an AS acting on behalf of an unregistered user, the S-CCF shall:

1) execute the procedures described in the steps 1, 2, 3, 4, 4A, 4B, 4C, 4D, 5, 6, 7, 8, 9, 10, 11, 12, 13,14,15 and 16 in the above paragraph (when the S-CCF receives, from a registered served user, an initial request for a dialog or a request for a standalone transaction).

NOTE 8: When the S-CCF does not have the user profile, before executing the actions as listed above, it initiates the S-CCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informs the HSS that the user is unregistered. The S-CCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14].

If the S-CCF fails to receive a SIP response or receives a 408 (Request Timeout) response or a 5xx response from the AS, the S-CCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION_CONTINUED" as specified in 3GPP TS 29.228 [14] or no default handling is indicated, execute the procedure from step 4; and

- if the default handling defined in the filter criteria indicates the value "SESSION_TERMINATED" as specified in 3GPP TS 29.228 [14], either forward the received response or, if the request is an initial INVITE request, send a 408 (Request Timeout) response or a 5xx response towards the served UE as appropriate (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

If the S-CCF receives any final response from the AS, it shall forward the response towards the served UE (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

When the S-CCF receives any response to the above request, the S-CCF may:

1) apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header, although the S-CCF shall not, except for the case where trust domain provisioning applies (e.g. response sent to an AS outside the trusted domain) as described in clause 4.4, modify or remove the priv-value set to "id" within the Privacy header.

NOTE 9: The P-Asserted-Identity header would normally only be expected in 1xx or 2xx responses.

NOTE 10: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

NOTE 10a: The priv-value “id” in the Privacy header will be used by the originating UE to distinguish the request of TIR by the terminating user as described in TS 183 008 [a].

When the S-CCF receives any response to the above request containing a term-ioi parameter, the S-CCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present, and remove all received ioi parameters from the forwarded response if next hop is not an AS.

NOTE 11: Any received term-ioi parameter will be a type 2 term-ioi or type 3 term-ioi. The term-ioi parameter identifies the sending network of the response message.

When the S-CCF receives any response to the above request, and forwards it to AS, the S-CCF shall insert a P-Charging-Vector header containing the orig-ioi parameter, if received in the request, and a type 3 term-ioi parameter in the response. The S-CCF shall set the type 3 term-ioi parameter to a value that identifies the sending network of the response and the type 3 orig-ioi parameter is set to the previously received value of type 3 orig-ioi.

When the S-CCF receives any 1xx or 2xx response to the initial request for a dialog, if the response corresponds to an INVITE request, the S-CCF 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-CCF, upon sending an initial INVITE request that includes an IP address in the SDP offer (in "c=" parameter), receives an error response indicating that the IP address type is not supported, (e.g., the S-CCF receives the 488 (Not Acceptable Here) with 301 Warning header indicating "incompatible network address format"), the S-CCF shall either:

- fork the initial INVITE request to the IBCF; or
- process the error response and forward it using the Via header.

When the S-CCF receives from the served user a target refresh request for a dialog, prior to forwarding the request the S-CCF shall:

1) remove its own URI from the topmost Route header;
2) create a Record-Route header containing its own SIP URI;
3) or INVITE dialogs (i.e. dialogs initiated by an INVITE request), save the Contact and Cseq header field values received in the request such that the S-CCF is able to release the session if needed;
4) in case the request is routed towards the destination user (Request-URI) or in case the request is routed to an AS located outside the trust domain, remove the 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-CCF receives any 1xx or 2xx response to the target refresh request for an INVITE dialog, the S-CCF shall replace the saved Contact and Record-Route header field values in the response such that the S-CCF is able to release the session if needed.

When the S-CCF receives from the served user a subsequent request other than a target refresh request for a dialog, prior to forwarding the request the S-CCF 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 in case the request 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.

With the exception of 305 (Use Proxy) responses, the S-CCF shall not recurse on 3xx responses.

5.4.3.3 Requests terminated at the served user

When the S-CCF receives, destined for a statically pre-configured PSI or a registered served user, an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CCF shall:

1) check if an original dialog identifier that the S-CCF previously placed in a Route header is present in the topmost Route header of the incoming request.
   - If present, the request has been sent from an AS in response to a previously sent request.

- If not present, it indicates that the request is visiting the S-CCF for the first time, and in this case the S-CCF 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-CCF shall reject the request by generating a 404 (Not Found) response. Otherwise, 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 then check whether the Request-URI matches the saved Request-URI. The Request-URI and saved Request-URI are considered a match if the Request-URI is equal to the saved value of the Request-URI, or if the Request-URI is a public GRUU and the saved value of the Request-URI is a temporary GRUU and both the public and temporary GRUUs represent the same public user identity and instance ID. 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-CCF 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 steps 10 through 14 from subclause 5.4.3.2) and skip the following steps.

3A) if the Request-URI is a GRUU, but is not valid as defined in subclause 5.4.7A.4, then return a 4xx response as specified in draft-ietf-sip-gruu [93];

3B) if the Request-URI contains a public GRUU and the saved value of the Request URI is a temporary GRUU, then replace the Request-URI with the saved value of the Request-URI;

3C) if the request contains a P-Asserted-Service header field check whether the IMS communication service identified by the ICSI value contained in the P-Asserted-Service header field is allowed by the subscribed services for the served user and if not remove the P-Asserted-Service header field;

3D) if the request does not contain a P-Asserted-Service header field check if the contents of the request matches a subscribed service (i.e. SDP media capabilities, Content-Type header field) for each and any of the subscribed services for the served user. As an operator option, if the contents of the request do not match a subscribed service, the S-CCF may reject the request by generating a 403 (Forbidden) response. Otherwise, continue with the rest of the steps;

3E) if the request does not contain a P-Asserted-Service header field and if the contents of the request are allowed by the subscribed services for the served user include a P-Asserted-Service header field in the request containing the ICSI value for the related IMS communication service, and use the as a header field in the initial request when matching initial filter criteria in step 4;

4) check whether the initial request matches the next unexecuted initial filter criteria based on the public user identity identified by the Request-URI in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then the S-CCF shall:

   - if the Request-URI is a temporary GRUU as defined in subclause 5.4.7A.3, then replace the Request-URI with the public GRUU that is associated with the temporary GRUU (i.e. the public GRUU representing the same public user identity and instance ID as the temporary GRUU);

   - 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

   - insert a type 3 orig-ioi parameter in the P-Charging-Vector header. The type 3 orig-ioi parameter identifies the sending network of the request message before the received orig-ioi. The S-CCF shall not include the type 3 term-ioi parameter;

NOTE 1: Depending on the result of the previous process, the S-CCF may contact one or more AS(s) before processing the outgoing Request-URI.

NOTE 2: If the Request-URI of the received terminating request contains a temporary GRUU, then step 4 replaces the Request-URI with the associated public GRUU before invoking the AS, and step 3B restores the original temporary GRUU when the request is returned from the AS.

NOTE 3: An AS can activate or deactivate its own filter criteria via the Sh interface. As the S-CCF checks initial filter criteria only on receipt of an initial request for a dialog, or a standalone transaction, a modified service profile will have no impact on transactions or dialogs already in progress and the modified profile will be effective only for new transactions and dialogs. If the S-CCF receives a modification of the iFC during their execution, then it should not update the stored initial Filter Criteria until the iFC related to the initial request have been completely executed.

5) if there was no original dialog identifier present in the topmost Route header 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-CCF 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 request store the value of the orig-ioi parameter received in the P-Charging-Vector header, if present, and remove all received ioi parameters from the forwarded request if next hop is not an AS;

NOTE 4: Any received orig-ioi parameter will be a type 2 orig-ioi. or type 3 orig-ioi. The orig-ioi parameter identifies the sending network of the request message. 8) in the case there are no Route headers in the request, create a target set of potential routes from the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2, as follows:

a) if the Request-URI is a valid GRUU as defined in subclause 5.4.7A.4, then the target set is determined by following the procedures for Request Targeting specified in draft-ietf-sip-gruu [93], using the public user identity and instance ID derived from the GRUU using the procedures of subclause 5.4.7A;

b) if the Request-URI is not a GRUU, then the target set is all the registered contacts saved for the destination public user identity;

9) if necessary perform the caller preferences to caller capabilities matching according to RFC 3841 [56B] to the target set;

NOTE 5: This might eliminate entries and reorder the target set.

10) in case there are no Route headers in the request:

a) if there is more than one route in the target set determined in steps 8) and 9) above:

- if the fork directive in the Request Disposition header was set to "no-fork", the contact with the highest qvalue parameter shall be used when building the Request-URI. In case no qvalue parameters were provided, the S-CCF shall decide locally what contact address to be used when building the Request-URI; otherwise

- fork the request or perform sequential search based on the relative preference indicated by the qvalue parameter of the Contact header in the original REGISTER request, as described in RFC3261 [26]. In case no qvalue parameters were provided, then the S-CCF determine the contact address to be used when building the Request-URI as directed by the Request Disposition header as described in RFC 3841 [56B]. If the Request-Disposition header is not present, the S-CCF shall decide locally whether to fork or perform sequential search among the contact addresses;

- in case that no route is chosen, return a 480 (Temporarily unavailable) response or another appropriate unsuccessful SIP response and terminate these procedures.

b) build a Request-URI with the contents of the Contact URI from the chosen route determined in the previous step;

c) insert a P-Called-Party-ID SIP header field containing the contents of the Request-URI received in the request unless the Request-URI contains a temporary GRUU in which case insert the public GRUU in the P-Called-Party-ID;

d) build the Route header field with the Path values from the chosen route; and

e) save the Request-URI and the total number of Record-route headers as part of the dialog request state.

NOTE 6: For each initial dialog request terminated at a served user two pieces of state are maintained to assist in processing GRUUs: the chosen contact address to which the request is routed; and the position of an entry for the S-CCF in the Record-Route header that will be responsible for GRUU translation, if needed (the position is the number of entries in the list before the entry was added). The entry will be added in step 5) of the below procedures for handling S-CCF receipt any 1xx or 2xx response to the initial request for a dialog. The S-CCF can record-route multiple times, but only one of those (the last) will be responsible for gruu translation at the terminating end.

11) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the S-CCF is able to release the session if needed;

12) optionally, apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header and privacy required by RFC 4244 [66] although the S-CCF shall not, except for the case where trust domain provisioning applies (e.g. request sent to an AS outside the trusted domain) as described in clause 4.4, modify or remove the priv-value set to "id" within the Privacy header;

NOTE 7: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

NOTE 7a: The priv-value "id" in the Privacy header will be used by the terminating UE to distinguish the request of OIR by the originating user as described in TS 183 007 [b].

13) in case of an initial request for a dialog, either:

- if the request is routed to an AS which is part of the trust domain, the S-CCF can decide whether to record-route or not. The decision is configured in the S-CCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CCF shall create a Record-Route header containing its own SIP URI; or

- if the request is routed elsewhere, create a Record-Route header containing its own SIP URI;

13A) if the request is routed to the P-CSCF remove the P-User-Database header if present; and

14) forward the request based on the topmost Route header.

If the S-CCF fails to receive a SIP response or receives a 408 (Request Timeout) response or a 5xx response from the AS, the S-CCF shall:

- if the default handling defined in the filter criteria indicates the value "SESSION_CONTINUED" as specified in 3GPP TS 29.228 [14] or no default handling is indicated, execute the procedure from step 4; and

- if the default handling defined in the filter criteria indicates the value "SESSION_TERMINATED" as specified in 3GPP TS 29.228 [14], either forward the received response or, if the request is an initial INVITE request, send a 408 (Request Timeout) response or a 5xx response towards the originating UE as appropriate (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

If the S-CCF receives any final response from the AS, it shall forward the response towards the originating UE (without verifying the matching of filter criteria of lower priority and without proceeding for further steps).

When the S-CCF receives any response to the above request and forwards it to AS, the S-CCF shall insert a P-Charging-Vector header containing the orig-ioi parameter, if received in the request, and a type 3 term-ioi parameter in the response. The S-CCF shall set the type 3 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.

NOTE 8: Any received term-ioi parameter will be a type 3 term-ioi. The term-ioi parameter identifies the service provider from which the response was sent.

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

1) Void.2) execute the procedures described in 1, 2, 3, 3C, 3D, 3E, 4, 5, 6, 7, 11, 13; 13A and 14 in the above paragraph (when the S-CCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

3) In case that no AS needs to be contacted, then S-CCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) and terminate these procedures.

NOTE 9: When the S-CCF does not have the user profile, before executing the actions as listed above, it initiates the S-CCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informs the HSS that the user is unregistered. The S-CCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14]. When requesting the user profile the S-CCF can include the information in the P-Private-Key header in S-CCF Registration/deregistration notification.

Prior to performing S-CCF Registration/Deregistration procedure with the HSS, the S-CCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14] or use the value as received in the P-User-Database header in the initial request for a dialog or a request for a standalone transaction as defined in RFC 4457 [82]. The HSS address received in the response to SLF query can be used to address the HSS of the public user identity with further queries.

When the S-CCF receives any 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-CCF is able to release the session if needed;

2) if the response is not forwarded to an AS (i.e. the response is related to a request that was matched to the first executed initial filter criteria), insert a type 2 term-ioi parameter in the P-Charging-Vector header of the outgoing response. The type 2 term-ioi is set 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. Values of orig-ioi and term-ioi in the received response are removed;

3) in the case where the S-CCF has knowledge that the SIP URI contained in the received P-Asserted-Identity header is an alias SIP URI for a tel URI the S-CCF shall add a second P-Asserted-Identity header containing this tel URI including the display name associated with the tel URI, if available. If the P-Asserted-Identity header contains only a tel URI, the S-CCF shall add a second P-Asserted-Identity header containing a SIP URI. The added SIP URI shall contain in the user part a "+" followed by the international public telecommunication number contained in tel URI, and user's home domain name in the hostport part. The added SIP URI shall contain the same value in the display name as contained in the tel URI. The S-CCF shall also add a user parameter equals "phone" to the SIP URI;

4) in case the response is sent towards the originating user, the S-CCF may remove the P-Access-Network-Info header based on local policy rules and the destination user (Request-URI); and

5) save an indication that GRUU routeing is to be performed for subsequent requests sent within this same dialog if:

   a) there is a record-route position saved as part of the initial dialog request state; and

   b) the contact address in the response is a valid GRUU as specified in subclause 5.4.7A.4.

NOTE 10: There could be several responses returned for a single request, and the decision to insert or modify the Record-Route needs to be applied to each. But a response might also return to the S-CCF multiple times as it is routed back through AS. The S-CCF will take this into account when carrying out step 5) to ensure that the information is stored only once.

When the S-CCF receives a response to a request for a standalone transaction (whether the user is registered or not), in the case where the S-CCF has knowledge that the SIP URI contained in the received P-Asserted-Identity header is an alias SIP URI for a tel URI the S-CCF shall add a second P-Asserted-Identity header containing this tel URI, including the display name associated with the tel URI, if available. If the P-Asserted-Identity header contains only a tel URI, the S-CCF shall add a second P-Asserted-Identity header containing a SIP URI. The added SIP URI shall contain in the user part a "+" followed by the international public telecommunication number contained in tel URI, and user's home domain name in the hostport part. The added SIP URI shall contain the same value in the display name as contained in the tel URI. The S-CCF shall also add a user parameter equals "phone" to the SIP URI. In case the response is forwarded to an AS that is located within the trust domain, the S-CCF shall retain the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header; otherwise, the S-CCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header.

When the S-CCF receives the 200 (OK) response for a standalone transaction request, the S-CCF shall:

1) insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CCF home network, including towards an AS; and

2) if the response is not forwarded to an AS (i.e. the response is related to a request that was matched to the first executed initial filter criteria),insert a type 2 term-ioi parameter in the P-Charging-Vector header of the outgoing response. The type 2 term-ioi is set to a value that identifies the sending network of the response and the type 2 orig-ioi parameter is set to the previously received value of orig-ioi.

NOTE 11: If the S-CCF forked the request of a stand alone transaction to multiple UEs and receives multiple 200 (OK) responses, the S-CCF will select and return only one 200 (OK) response. The criteria that the S-CCF employs when selecting the 200 (OK) response is based on the operator's policy (e.g. return the first 200 (OK) response that was received).

When the S-CCF receives, destined for a served user, a target refresh request for a dialog, prior to forwarding the request, the S-CCF shall:

1) if the incoming request is received on a dialog for which GRUU routeing is to be performed and the Request-URI is not the GRUU for this dialog, then return a response of 400 (Bad Request).

2) if the incoming request is received on a dialog for which GRUU routeing is to be performed and the Request-URI contains the GRUU for this dialog then the S-CCF shall:

   - perform the procedures for Request Targeting specified in draft-ietf-sip-gruu [93], using the public user identity and instance ID derived from the Request-URI, as specified in subclause 5.4.7A;

   - if no contact can be selected, return a response of 480 (Temporarily Unavailable).

3) remove its own URI from the topmost Route header;

4) for INVITE dialogs (i.e. dialogs initiated by an INVITE request), save the Contact and Cseq header field values received in the request such that the S-CCF is able to release the session if needed;

5) create a Record-Route header containing its own SIP URI; and

6) forward the request based on the topmost Route header.

When the S-CCF receives any 1xx or 2xx response to the target refresh request for a dialog (whether the user is registered or not), the S-CCF shall:

1) for INVITE dialogs, replace the saved Contact header field values in the response such that the S-CCF 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-CCF shall retain the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header; otherwise, the S-CCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header.

When the S-CCF receives, destined for the served user, a subsequent request other than target refresh request for a dialog, prior to forwarding the request, the S-CCF shall:

1) if the incoming request is received on a dialog for which GRUU routeing is to be performed and the Request-URI is not the GRUU for this dialog, then return a response of 400 (Bad Request).

2) if the incoming request is received on a dialog for which GRUU routeing is to be performed and the Request-URI contains the GRUU for this dialog then the S-CCF shall:

   - perform the procedures for Request Targeting specified in draft-ietf-sip-gruu [93], using the public user identity and instance ID derived from the Request-URI, as specified in subclause 5.4.7A;

   - if no contact can be selected, return a response of 480 (Temporarily Unavailable).

3) remove its own URI from the topmost Route header; and

4) forward the request based on the topmost Route header.

When the S-CCF receives a response to a subsequent request other than target refresh request for a dialog, in case the response is forwarded to an AS that is located within the trust domain, the S-CCF shall retain the P-Access-Network-Info header and the access-network-charging-info parameter from the P-Charging-Vector header; otherwise, the S-CCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter from the P-Charging-Vector header.

With the exception of 305 (Use Proxy) responses, the S-CCF shall not recurse on 3xx responses.

5.10.6 Screening of SIP signalling

5.10.6.1 General

The IBCF may act as a B2BUA when it performs screening of SIP signalling functionality. In this case the B2BUA behaviour of the IBCF shall comply with the description given in subclause 5.10.5 for the IMS-ALG functionality.

NOTE: Many headers are intended for end-to-end operation; removal of such headers will impact the intended end-to-end operation between the end users. Additionally the IM CN subsystem does not preclude security mechanisms covering SIP headers; any such removal ~~can~~ may prevent validation of all headers covered by the security mechanism. Further study in release 2 will be given to specifying procedures that can act in a more transparent manner to the end user for some of these screening functions, and therefore allow the screening function to use proxy behaviour. Use of draft-ietf-sipping-media-policy-dataset, draft-hilt-sipping-policy-package, draft-hilt-sipping-policy-usecases, draft-hilt-sipping-session-policy-framework, draft-hilt-sipping-session-spec-policy, and draft-camarillo-sipping-sbc-funcs will be investigated for this purpose.

5.10.6.2 IBCF procedures for SIP headers

If specified by local policy rules, the IBCF may omit or modify any other received SIP headers prior to forwarding SIP messages, with the following exceptions.

As a result of any screening policy adopted, the IBCF should not modify at least the following headers which would cause mis-operation of the IM CN subsystem:

- Authorization; and
- WWW-Authenticate.

Where the IBCF appears in the path between the UE and the S-CCF, some headers are involved in the registration and authentication of the user. As a result of any screening policy adopted as part of normal operation, e.g. where the request or response is forwarded on, the IBCF should not modify as part of the registration procedure at least the following headers:

- Path; and
- Service-Route.

NOTE 1: If the IBCF modifies SIP information elements (SIP headers, SIP message bodies) other than as specified by SIP procedures (e.g., RFC 3261 [26]) caution needs to be taken that SIP functionality (e.g., routeing using Route, Record-Route and Via) is not impacted in a way that could create interoperability problems with networks that assume that this information is not modified.

NOTE 2: Where operator requirements can be achieved by configuration hiding, then these procedures can be used in preference to screening.

The IBCF may add, remove, or modify, the P-Early-Media header within forwarded SIP requests and responses according to procedures in draft-ejzak-sipping-p-em-auth [109].

NOTE 3: The IBCF can use the header for the gate control procedures, as described in 3GPP TS 29.214 [13D]. In the presence of early media for multiple dialogs due to forking, if the IBCF is able to identify the media associated with a dialog, (i.e., if symmetric RTP is used by the UE and the IBCF can use the remote SDP information to determine the source of the media) the IBCF can selectively open the gate corresponding to an authorized early media flow for the selected media.

5.10.6.3 IBCF procedures for SIP message bodies

If IP address translation (NA(P)T or IP version interworking) occurs on the user plane, the IBCF shall modify SDP according to the corresponding annex F and G~~ as appropriate.~~

Additionally, the IBCF may take the followings action upon SIP message bodies:

1) examine the length of a SIP message body and if required by local policy, and take an appropriate action (e.g. forward the message body transparently, reject the request, remove the body);

2) examine the characteristics of the message body (i.e. check the values of any "Content-Type", "Content-Disposition", and "Content-Language" headers), take an appropriate action defined by local policy (e.g. forward the body unchanged, remove the body, reject the call); and

3) examine the content of SIP bodies, and take appropriate action defined by local policy (e.g. forward the body unchanged, remove the body, reject the call).

6 Application usage of SDP

6.1.1 General

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 [30] as updated by RFC 4032 [64].

In order to authorize the media streams, the P-CSCF and S-CCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261 [26].

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, and if the RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556 [56], then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 [56] to specify the required bandwidth allocation for RTCP.

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 29.213 [13C].

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 2833 [23].

In case if the IP-CAN requires any access specific procedures, 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 appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

In order to fulfil the QoS requirements of one or more media streams, the UE may re-use previously reserved resources. In this case the local preconditions related to the media stream, for which resources are re-used, shall be indicated as met.

If an IP-CAN bearer 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].

NOTE 3: The UE can use one IP address for signalling (and specify it in the Contact header) and different IP address(es) for media (and specify it in the "c=" parameter of the SDP).

If the UE wants to transport media streams with TCP and there are no specific alternative negotiation mechanisms defined for that particular application, then the UE shall support the procedures and the SDP rules specified in RFC 4145 [83].

6.2 Procedures at the P-CSCF

When the P-CSCF receives any SIP request containing an SDP offer, 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 specified in RFC 3261 [26]. The P-CSCF shall order the SDP payload with the most preferred codec listed first. If the SDP offer is encrypted, the P-CSCF may reject the request.

When the P-CSCF receives a SIP response different from 200 (OK) response containing an SDP offer, the P-CSCF shall not examine the media parameters in the received SDP offer, but the P-CSCF shall rather check the succeeding request containing the SDP answer for this offer, and if necessary (i.e. the SDP answer reduced by the UE still breaches local policy), the P-CSCF shall return a 488 (Not Acceptable Here) response containing the local policy allowed SDP payload. If the SDP answer is encrypted, the P-CSCF may reject the succeeding request.

When the P-CSCF receives a 200 (OK) response containing SDP offer, the P-CSCF shall examine the media parameters in the received SDP. If the P-CSCF finds any media parameters which are not allowed on the network by local policy, the P-CSCF shall forward the SDP offer and on the receipt of the ACK request containing the SDP answer, it shall immediately terminate the session as described in subclause 5.2.8.1.2. If the SDP offer is encrypted, the P-CSCF shall forward the SDP offer and on the receipt of the ACK request containing the SDP answer, it may immediately terminate the session as described in subclause 5.2.8.1.2.

When the P-CSCF receives any SIP request containing an SDP offer for which resource authorization procedure over the Gq' interface is required (e.g. in case the P-CSCF is serving a UE connected to a fixed broadband access), upon receipt of an indication over the Gq' interface that the requested resources for a multimedia session currently being established cannot be granted (e.g. AA-Answer message from SPDF with appropriate reservation failure indication), the P-CSCF shall terminate this received request and answer it with a 500 (Server Internal Error) response.

When the P-CSCF receives a 200 (OK) response containing an SDP offer, for which resource authorization procedure over the Gq' interface is required (e.g. in case the P-CSCF is serving a UE connected to a fixed broadband access), upon receipt of an indication over the Gq' interface that the requested resources for a multimedia session currently being established cannot be granted (e.g. AA-Answer message from SPDF with appropriate reservation failure indication), the P-CSCF shall check the SIP message containing the SDP answer for this SDP offer, and if necessary (i.e. a new indication that resources cannot be granted is received by the P-CSCF over the Gq' interface), the P-CSCF shall terminate the session as described in subclause 5.2.8.1.2.

In case a device performing address and/or port number conversions is provided by a NA(P)T or NA(P)t-PT controlled by the P-CSCF, or by a hosted NAT, located along the media path, the P-CSCF may need to modify the media connection data in SDP bodies according to the procedures described in F and/or annex G.

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. 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.

7 Extensions within the present document

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 particular access technologies.

7.2A.4.2 Syntax

The syntax of the P-Access-Network-Info header is described in RFC 3455 [52]. There are additional coding rules for this header depending on the type of IP-CAN, according to access technology specific descriptions.

Table 7.6A describes 3GPP-specific extended syntax of the P-Access-Network-Info header field defined in RFC 3455 [52].

Table 7.6A: Syntax of extended P-Access-Network-Info header

```
P-Access-Network-Info  = "P-Access-Network-Info" HCOLON
                         access-net-spec *(COMMA access-net-spec)
access-net-spec        = access-type ~~[SEMI np]~~ *(SEMI access-info)
access-type            = "IEEE-802.11" / "IEEE-802.11a" / "IEEE-802.11b" / "IEEE-802.11g" /
                         "3GPP-GERAN" / "3GPP-UTRAN-FDD" / "3GPP-UTRAN-TDD" / "ADSL" / "ADSL2" /
                         "ADSL2+" / "RADSL" / "SDSL" / "HDSL" / "HDSL2" / "G.SHDSL" / "VDSL" /
                         "IDSL" / "3GPP2-1X" / "3GPP2-1X-HRPD" /token
~~np                    = "network-provided"~~
access-info            = cgi-3gpp / utran-cell-id-3gpp / dsl-location / np / i-wlan-node-id / ci-
      3gpp2/ extension- access-info
extension-access-info  = gen-value
cgi-3gpp               = "cgi-3gpp" EQUAL (token / quoted-string)
utran-cell-id-3gpp     = "utran-cell-id-3gpp" EQUAL (token / quoted-string)
i-wlan-node-id         = "i-wlan-node-id" EQUAL (token / quoted-string)
dsl-location           = "dsl-location" EQUAL (token / quoted-string)
np                     = "network-provided"
ci-3gpp2               = "ci-3gpp2" EQUAL (token / quoted-string)
```

NOTE: Addition of the P-Access-Network-Info header by proxies, and repetition of the P-Access-Network-Info header within the same request or response, requires an update to RFC 3455 before such usage is valid.

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

~~The UE~~Entities inserting the P-Access-Network-Info header shall populate the P-Access-Network-Info header, where use is specified in subclause 5.1 and subclause 5.2, with the following contents:

1) the access-type field set to one of "3GPP-GERAN","3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b" "IEEE-802.11g", "ADSL", "ADSL2", "ADSL2+", "RADSL", "SDSL", "HDSL", "HDSL2", "G.SHDSL", "VDSL", "IDSL" or "DOCSIS" as appropriate to the access technology in use.

2) if the access type field is set to "3GPP-GERAN", a cgi-3gpp parameter set to the Cell Global Identity obtained from lower layers of the UE. The Cell Global Identity is a concatenation of MCC, MNC, LAC and CI (as described in 3GPP TS 23.003 [3]). The value of "cgi-3gpp" parameter is therefore coded as a text string as follows:

   Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and CI (fixed length code of 16 bits using a full hexadecimal representation);

3) if the access type field is equal to "3GPP-UTRAN-FDD", or "3GPP-UTRAN-TDD", a "utran-cell-id-3gpp" parameter set to a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003 [3]) and the UMTS Cell Identity (as described in 3GPP TS 25.331 [9A]), obtained from lower layers of the UE, and is coded as a text string as follows:

   Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and UMTS Cell Identity (fixed length code of 28 bits);

4) if the access type field is set to "3GPP2-1X", a ci-3gpp2 parameter set to the ASCII representation of the hexadecimal value of the string obtained by the concatenation of SID (16 bits), NID (16 bits), PZID (8 bits) and BASE_ID (16 bits) (see 3GPP2 C.S0005-D [85]) in the specified order. The length of the ci-3gpp2 parameter shall be 14 hexadecimal characters. The hexadecimal characters (A through F) shall be coded using the uppercase ASCII characters. If the MS does not know the values for any of the above parameters, the MS shall use the value of 0 for that parameter. For example, if the SID is unknown, the MS shall represent the SID as 0x0000;

NOTE 1: The SID value is represented using 16 bits as supposed to 15 bits as specified in 3GPP2 C.S0005-D [85].

EXAMPLE: If SID = 0x1234, NID = 0x5678, PZID = 0x12, BASE_ID = 0xFFFF, the ci-3gpp2 value is set to the string "1234567812FFFF".

5) if the access type field is set to "3GPP2-1X-HRPD", a ci-3gpp2 parameter set to the ASCII representation of the hexadecimal value of the string obtained by the concatenation of Sector ID (128 bits) and Subnet length (8 bits) (see 3GPP2 C.S0024-A [86]) in the specified order. The length of the ci-3gpp2 parameter shall be 34 hexadecimal characters. The hexadecimal characters (A through F) shall be coded using the uppercase ASCII characters;

EXAMPLE: If the Sector ID = 0x12341234123412341234123412341234, Subnet length = 0x11, the ci-3gpp2 value is set to the string "12341234123412341234123412341234123411".

6) if the access-type field set to one of "IEEE-802.11", "IEEE-802.11a", "IEEE-WLAN-802.11b" or "IEEE-802.11g", an "i-wlan-node-id" parameter is set to the MAC address of the AP.

7) If the access-type field is set to one of "ADSL", "ADSL2", "ADSL2+", "RADSL", "SDSL", "HDSL", "HDSL2", "G.SHDSL", "VDSL", "IDSL", the access-info field shall contain a dsl-location parameter obtained from the CLF (see NASS functional architecture) ; and 8) if the access-type field set to "DOCSIS", the access info parameter is set to a null value. This release of this specification does not define values for use in this parameter.

NOTE 2: The "cgi-3gpp", the "utran-cell-id-3gpp", the "ci-3gpp2", the "i-wlan-node-id", and the "dsl-location" parameters described above among other usage also constitute the location identifiers that are used for IMS emergency services.

If the P-CSCF receives an initial request for a dialog or standalone transaction or an unknown method and:

- the request includes a P-Access-Network-Info header with a "network-provided" parameter the P-CSCF shall remove the P-Access-Network-Info header;

- the request is sent using xDSL as an IP-CAN the P-CSCF may insert a P-Access-Network-Info header into the request by setting the access-type field to one of "ADSL", "ADSL2", "ADSL2+", "RADSL", "SDSL", "HDSL", "HDSL2", "G.SHDSL", "VDSL", or "IDSL", adding the "network-provided" parameter and the "dsl-location" parameter with the value received in the Location-Information header in the User-Data Answer command as specified in ETSI ES 283 035 [98]; and

NOTE 3: The way the P-CSCF deduces that the request comes using xDSL access is implementation dependent.

Editor's Note: Insertion of P-Access-Network-Info header by a P-CSCF is not allowed according to RFC 3455 [52].

- the request is sent using DOCSIS as an IP-CAN the P-CSCF may insert a P-Access-Network-Info header into the request by setting the access-type field to "DOCSIS" and including the "network-provided" parameter.

NOTE 4: The way the P-CSCF deduces that the request comes using DOCSIS access is implementation dependent.

Editor's Note: Insertion of P-Access-Network-Info header by a P-CSCF is not allowed according to RFC 3455 [52].

Annex A Profiles of IETF RFCs for ~~3GPP~~ ETSI TISPAN usage

A.2.1.2 Major capabilities

Editor's note: it needs to be checked whether it should be explicitly clarified that the IBCF (IMS-ALG) is transparent to some presence or conference extensions.

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	o	c3
2	registrar?	[26] subclause 10.3	o	c4
2A	registration of multiple contacts for a single address of record	[26] 10.2.1.2, 16.6	o	o
2B	initiating a session?	[26] subclause 13	o	o
2C	initiating a session which require local and/or remote resource reservation?	[27]	o	c43
3	client behaviour for INVITE requests?	[26] subclause 13.2	c18	c18
4	server behaviour for INVITE requests?	[26] subclause 13.3	c18	c18
5	session release?	[26] subclause 15.1	c18	c18
6	timestamping of requests?	[26] subclause 8.2.6.1	o	o
7	authentication between UA and UA?	[26] subclause 22.2	c34	c34
8	authentication between UA and registrar?	[26] subclause 22.2	o	n/a
8A	authentication between UA and proxy?	[26] 20.28, 22.3	o	o
9	server handling of merged requests due to forking?	[26] 8.2.2.2	m	m
10	client handling of multiple responses due to forking?	[26] 13.2.2.4	m	m
11	insertion of date in requests and responses?	[26] subclause 20.17	o	o
12	downloading of alerting information?	[26] subclause 20.4	o	o
	Extensions			
13	the SIP INFO method?	[25]	o	n/a
14	reliability of provisional responses in SIP?	[27]	c19	c44
15	the REFER method?	[36]	o	c33
16	integration of resource management and SIP?	[30] [64]	c19	c44
17	the SIP UPDATE method?	[29]	c5	c44
19	SIP extensions for media authorization?	[31]	o	c14
20	SIP specific event notification?	[28]	o	c13
21	the use of NOTIFY to establish a dialog?	[28] 4.2	o	n/a
22	acting as the notifier of event information?	[28]	c2	c15
23	acting as the subscriber to event information?	[28]	c2	c16
24	session initiation protocol extension header field for registering non-adjacent contacts?	[35]	o	c6
25	private extensions to the Session Initiation Protocol (SIP) for network asserted identity within trusted networks?	[34]	o	m
26	a privacy mechanism for the Session Initiation Protocol (SIP)?	[33]	o	m
26A	request of privacy by the inclusion of a Privacy header indicating any privacy option?	[33]	c9	c11
26B	application of privacy based on the received Privacy header?	[33]	c9	n/a
26C	passing on of the Privacy header transparently?	[33]	c9	c12

Item	Does the implementation support	Reference	RFC status	Profile status
26D	application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the assistance of intermediaries are obscured?	[33] 5.1	c10	c27
26E	application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs?	[33] 5.2	c10	c27
26F	application of the privacy option "user" such that user level privacy functions are provided by the network?	[33] 5.3	c10	c27
26G	application of the privacy option "id" such that privacy of the network asserted identity is provided by the network?	[34] 7	c10	n/a
26H	application of the privacy option "history" such that privacy of the History-Info header is provided by the network?	[66] 7.2	c37	c37
27	a messaging mechanism for the Session Initiation Protocol (SIP)?	[50]	o	c7
28	session initiation protocol extension header field for service route discovery during registration?	[38]	o	c17
29	compressing the session initiation protocol?	[55]	o	c8
30	private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)?	[52]	o	m
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]	o	c20
38	the Reason header field for the session initiation protocol?	[34A]	o	o (note 1)
39	an extension to the session initiation protocol for symmetric response routeing?	[56A]	o	~~x~~o
40	caller preferences for the session initiation protocol?	[56B]	C29	c29
40A	the proxy-directive within caller-preferences?	[56B] 9.1	o.5	o.5
40B	the cancel-directive within caller-preferences?	[56B] 9.1	o.5	o.5
40C	the fork-directive within caller-preferences?	[56B] 9.1	o.5	c28
40D	the recurse-directive within caller-preferences?	[56B] 9.1	o.5	o.5
40E	the parallel-directive within caller-preferences?	[56B] 9.1	o.5	c28
40F	the queue-directive within caller-preferences?	[56B] 9.1	o.5	o.5
41	an event state publication extension to the session initiation protocol?	[70]	o	c30
42	SIP session timer?	[58]	c19	c19
43	the SIP Referred-By mechanism?	[59]	o	c33
44	the Session Initiation Protocol (SIP) "Replaces" header?	[60]	c19	c38 (note 1)

Item	Does the implementation support	Reference	RFC status	Profile status
45	the Session Initiation Protocol (SIP) "Join" header?	[61]	c19	c19 (note 1)
46	the caller capabilities?	[62]	o	c35
47	an extension to the session initiation protocol for request history information?	[66]	o	o
48	Rejecting anonymous requests in the Session Initiation Protocol (SIP)	[67]	o	o
49	session initiation protocol URIs for applications such as voicemail and interactive voice response	[68]	o	o
50	Session Initiation Protocol's (SIP) non-INVITE transactions?	[84]	m	m
51	the P-User-Database private header extension?	[82] 4	o	o
52	a uniform resource name for services	[69]	n/a	c39
53	obtaining and using GRUUs in the Session Initiation Protocol (SIP)	[93]	o	c40 (note 2)
54	an extension to the session initiation protocol for request cpc information?	[95]	o (note 3)	c41
55	the Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)?	[96]	o	c42
56	the SIP P-Profle-Key private header extension?	[97]	n/a	n/a
57	managing client initiated connections in SIP?	[92]	o	c45
58	indicating support for interactive connectivity establishment in SIP?	[102]	o	c46
59	multiple-recipient MESSAGE requests in the session initiation protocol?	[104]	c47	c48
60	SIP location conveyance	[89]	o	c49
61	referring to multiple resources in the session initiation protocol?	[105]	c50	c50
62	conference establishment using request-contained lists in the session initiation protocol?	[106]	c51	c52
63	subscriptions to request-contained resource lists in the session initiation protocol?	[107]	c53	c53
64	dialstring parameter for the session initiation protocol uniform resource identifier?	[103]	o	c19
65	the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular?	[111]	o	c60
66	the SIP P-Early-Media private header extension for authorization of early media?	[109] 8	o	c58
71	addressing an amplification vulnerability in session initiation protocol forking proxies?	[117]	n/a	n/a
72	the remote application identification of applying signalling compression to SIP	[79] 9.1	o	c8
73	a session initiation protocol media feature tag for MIME application sub-types?	[120]	o	c59
74	Identification of communication services in the session initiation protocol?	[121]	o	c61
75	XML Schema for PSTN?	[ANNEX ZB]	m	c62

Item	Does the implementation support	Reference	RFC status	Profile status
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-CCF functional entity.			
c4:	IF A.3/4 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - S-CCF 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-CCF or UE.			
c7:	IF A.3/1 OR A.3/4 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9B THEN m ELSE n/a - - UA or S-CCF or AS acting as terminating UA or AS acting as originating UA or AS performing 3rd party call control or IBCF (IMS-ALG).			
c8:	IF A.3/1 THEN (IF (A.3B/1 OR A.3B/2 OR A.3B/3 OR A.3B/4 OR A.3B/5 OR A.3B/11 OR A.3B/12 OR A.3B/13 OR A.3B/14) THEN m ELSE o) ELSE n/a - - UE behaviour (based on P-Access-Network-Info usage).			
c9:	IF A.4/26 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).			
c10:	IF A.4/26B THEN o.3 ELSE n/a - - application of privacy based on the received Privacy header.			
c11:	IF A.3/1 OR A.3/6 THEN o ELSE IF A.3/9B THEN m ELSE n/a - - UE or MGCF, IBCF(IMS-ALG).			
c12:	IF A.3/7D THEN m ELSE n/a - - AS performing 3rd-party call control.			
c13:	IF A.3/1 OR A.3/2 OR A.3/4 OR A.3/9B THEN m ELSE o - - UE or S-CCF or IBCF (IMS-ALG).			
c14:	IF A.3/1 AND ~~A4/2B~~ (A.3B/1 OR A.3B/2 OR A.3B/3 OR A.3B/4 OR A.3B/5) THEN m ELSE ~~IF A.3/2 THEN o ELSE~~ n/a – UE with appropriate access technology ~~and initiating sessions or P-CSCF~~.			
c15:	IF A.4/20 AND (A.3/4 OR A.3/9B) THEN m ELSE o – SIP specific event notification extensions and S-CCF or IBCF (IMS-ALG).			
c16:	IF A.4/20 AND (A.3/1 OR A.3/2 OR A.3/9B) THEN m ELSE o - - SIP specific event notification extension and UE or P-CSCF or IBCF (IMS-ALG).			
c17:	IF A.3/1 or A.3/4 THEN m ELSE n/a - - UE or S-CCF			
c18:	IF A.4/2B THEN m ELSE n/a - - initiating sessions.			
c19:	IF A.4/2B THEN o ELSE n/a - - initiating sessions.			
c20:	IF A.3/1 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-CCF 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-CCF.			
c25:	IF A.4/30 AND (A.3/1 OR A.3/4 OR A.3/7A OR A.3/7D OR A.3/9B) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE, S-CCF or AS acting as terminating UA or AS acting as third-party call controller or IBCF (IMS-ALG).			
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.			
c28:	IF A.3/1 THEN m ELSE o.5 - - UE.			
c29:	IF A.4/40A OR A.4/40B OR A.4/40C OR A.4/40D OR A.4/40E OR A.4/40F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol.			
c30:	IF A.3A/1 OR A.3A/2 THEN m ELSE IF A.3/1 THEN o ELSE n/a - - presence server, presence user agent, UE, AS.			
c33:	IF A.3/9B OR A.3 A /11 OR A.3 A /12 OR A.4/44 THEN m ELSE o - - BCF (IMS-ALG) or conference focus or conference participant or the Session Initiation Protocol (SIP) "Replaces" header.			
c34:	IF A.4/44 OR A.4/45 OR A.3/9B THEN m ELSE n/a - - the Session Initiation Protocol (SIP) "Replaces" header or the Session Initiation Protocol (SIP) "Join" header or IBCF (IMS-ALG).			
c35:	IF A.3/4 OR A.3/9 B OR A.3A/21 OR A.3A/22 THEN m ELSE IF (A.3/1 OR A.3/6 OR A.3/7 OR A.3/8) THEN o ELSE n/a - - S-CCF or BCF (IMS-ALG) functional entities or CSI user agent or CSI application server, UE or MGCF or AS or MRFC functional entity.			
c37	IF A.4/47 THEN o.3 ELSE n/a - - an extension to the session initiation protocol for request history information.			
c38:	IF A.4/2B AND (A.3A/11 or A.3A/12 or A.3/7D) THEN m ELSE IF A.4/2B THEN o ELSE n/a - - initiating sessions, conference focus, conference participant, AS performing 3rd party call control.			
c39:	IF A.3/1 THEN m ELSE n/a - - UE.			
c40	IF A.3/4 OR A.3/1 THEN m ELSE IF (A.3/7A OR A.3/7B OR A.3/7D) THEN o ELSE n/a - - S-CCF, UE, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control.			
c41:	IF A.3/2 OR A.3/3 OR A.3/4 OR A.3.5 OR A.3/6 OR A.3/7 OR A.3/8 OR A.3/9 THEN o ELSE n/a - - cpc URI parameter.			
c42:	IF A.3/1 n/a ELSE o - - UE.			
c43:	IF A.4/2B THEN o ELSE n/a - - initiating sessions.			
c44:	IF A.4/2C THEN m ELSE o - - initiating a session which require local and/or remote resource reservation.			
c45:	IF A.3/1 OR A.3/2 OR A.3/4 THEN o ELSE n/a - - UE, S-CCF functional entity.			

Item	Does the implementation support	Reference	RFC status	Profile status
c46	IF A.3/1 OR A.3/2 OR A.3/4 THEN o ELSE n/a - - UE, S-CCF functional entity.			
c47:	IF A.4/27 THEN o ELSE n/a - - a messaging mechanism for the Session Initiation Protocol (SIP).			
c48:	IF A.3A/32 AND A.4/27 THEN m ELSE IF A.4/27 THEN o ELSE n/a - - messaging list server, a messaging mechanism for the Session Initiation Protocol (SIP).			
c49:	IF A.3/1 OR A.3/9B THEN m ELSE o - - UE, IBCF (IMS-ALG).			
c50:	IF A.4/15 THEN o ELSE n/a - - the REFER method.			
c51:	IF A.4/2B THEN o ELSE n/a - - initiating a session.			
c52:	IF A.3A/11 AND A.4/2B THEN m ELSE IF A.4/2B THEN o ELSE n/a - - conference focus, initiating a session.			
c53:	IF A.4/20 THEN o ELSE n/a - - SIP specific event notification.			
c58:	IF A.3/9B OR A.3/6 THEN m ELSE o - - IBCF (IMS-ALG), MGCF.			
c59:	IF (A.3/4 THEN m ELSE IF (A.3/1 OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/8) THEN o ELSE n/a - - S-CCF, UE, MGCF, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, or MRFC.			
c60:	IF A.3/9B THEN m ELSE IF A.3/1 OR A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE n/a - - IBCF (IMS-ALG), UE, AS acting as terminating UA, AS acting as originating UA, AS performing 3rd party call control.			
c61:	IF (A.3/1 OR A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/8 OR A.3/9B) THEN o ELSE n/a - - UE, MGCF, AS, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, or MRFC or IBCF (IMS-ALG).o.1: At least one of these capabilities is supported.			
c62:	IF A.3/6 OR A.3/7A OR A.3/7B OR A.3/7D THEN o ELSE IF A.3/9B THEN o ELSE n/a - - MGCF, AS acting as terminating UA, or redirect server, AS acting as originating UA, AS performing 3rd party call control, IBCF (IMS-ALG).			
o.2:	At least one of these capabilities is supported.			
o.3:	At least one of these capabilities is supported.			
o.4:	At least one of these capabilities is supported.			
o.5:	At least one of these capabilities is supported.			
NOTE 1:	At the MGCF, the interworking specifications do not support a handling of the header associated with this extension.			
NOTE 2:	If a UE is unable to become engaged in a service that potentially requires the ability to identify and interact with a specific UE even when multiple UEs share the same single Public User Identity then the UE support can be "o" instead of "m". Examples include telemetry applications, where point-to-point communication is desired between two users.			
NOTE 3:	It has to be clarified within the draft that the cpc value belongs to the trust domain and shall not be populated by UE's.			

Prerequisite A.5/20 - - SIP specific event notification

Table A.4A: Supported event packages

Item	Does the implementation support	Subscriber			Notifier		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	reg event package?	[43]	c1	c3	[43]	c2	c4
1A	reg event package extension for GRUUs?	[94]	c1	c25	[94]	c2	c4
2	refer package?	[36] 3	c13	c13	[36] 3	c13	c13
3	presence package?	[74] 6	c1	c5	[74] 6	c2	c6
4	event list with underlying presence package?	[75], [74] 6	c1	c7	[75], [74] 6	c2	c8
5	presence.winfo template-package?	[72] 4	c1	c9	[72] 4	c2	c10
6	ua-profile package?	[77] 3	c1	c11	[77] 3	c2	c12
7	conference package?	[78] 3	c1	c21	[78] 3	c1	c22
8	message-summary package?	[65]	c1	c23	[65] 3	c2	c24
9	poc-settings package	[110]	c1	c26	[110]	c2	c27

c1: IF A.4/23 THEN o ELSE n/a - - acting as the subscriber to event information.
c2: IF A.4/22 THEN o ELSE n/a - - acting as the notifier of event information.
c3: IF A.3/1 OR A.3/2 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - UE, P-CSCF, AS.
c4: IF A.3/4 THEN m ELSE n/a - - S-CCF.
c5: IF A.3A/3 OR A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - resource list server or watcher, acting as the subscriber to event information.
c6: IF A.3A/1 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server, acting as the notifier of event information.
c7: IF A.3A/4 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - watcher, acting as the subscriber to event information.
c8: IF A.3A/3 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - resource list server, acting as the notifier of event information.
c9: IF A.3A/2 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - presence user agent, acting as the subscriber to event information.
c10: IF A.3A/1 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server, acting as the notifier of event information.
c11: IF A.3A/2 OR A.3A/4 THEN o ELSE IF A.4/23 THEN o ELSE n/a - - presence user agent or watcher, acting as the subscriber to event information.
c12: IF A.3A/1 OR A.3A/3 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - presence server or resource list server, acting as the notifier of event information.
c13: IF A.4/15 THEN m ELSE n/a - - the REFER method.
c21: IF A.3A/12 THEN m ELSE IF A.4/23 THEN o ELSE n/a - - conference participant or acting as the subscriber to event information.
c22: IF A.3A/11 THEN m ELSE IF A.4/22 THEN o ELSE n/a - - conference focus or acting as the notifier of event information.
c23: IF (A.3/1 OR A.3/7A OR A.3/7B) AND A.4/23 THEN o ELSE n/a - - UE, AS acting as terminating UA, or redirect server, AS acting as originating UA all as subscriber of event information.
c24: IF (A.3/1 OR A.3/7A OR A.3/7B) AND A.4/22 THEN o ELSE n/a - - UE, AS acting as terminating UA, or redirect server, AS acting as originating UA all as notifier of event information.
c25: IF A.4A/1 THEN (IF A.3/1 AND A.4/53 THEN m ELSE o) ELSE n/a - - reg event package, UE, reg event package extension for GRUUs.
c26: IF (A.3/7B OR A.3/1) AND (A.4/23 OR A.4/41) THEN o ELSE n/a - - AS acting as originating UA, UE ,acting as the subscriber to event information, an event state publication extension to the session initiation protocol.
c27: IF (A.4/22 OR A.4/41) AND A.3/1 THEN o ELSE n/a - - UE, acting as the notifier of event information, an event state publication extension to the session initiation protocol.

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	o	o	[26] 20.1	m	m
1A	Accept-Contact	[56B] 9.2	c24	c24	[56B] 9.2	c32	c32
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
4	Alert-Info	[26] 20.4	o	o	[26] 20.4	c1	c1
5	Allow	[26] 20.5, [26] 5.1	o (note 1)	o	[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	o	o	[26] 20.9	o	o
11	Contact	[26] 20.10	m	m	[26] 20.10	m	m
12	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
13	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
14	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
15	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
16	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
17	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
18	Date	[26] 20.17	c4	c4	[26] 20.17	m	m
19	Expires	[26] 20.19	o	o	[26] 20.19	o	o
20	From	[26] 20.20	m	m	[26] 20.20	m	m
20A	Geolocation	[89] 3.2	c33	c33	[89] 3.2	c33	c33
20B	History-Info	[66] 4.1	c31	c31	[66] 4.1	c31	c31
21	In-Reply-To	[26] 20.21	o	o	[26] 20.21	o	o
21A	Join	[61] 7.1	c30	c30	[61] 7.1	c30	c30
22	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
23	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
23A	Min-SE	[58] 5	c26	c26	[58] 5	c25	c25
24	Organization	[26] 20.25	o	o	[26] 20.25	o	o
24A	P-Access-Network-Info	[52] 4.4	c15	c16	[52] 4.4	c15	c17
24B	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	c7	c7
24C	P-Asserted-Service	[121] 4.1	n/a	n/a	[121] 4.1	c38	c38
24D	P-Called-Party-ID	[52] 4.2	x	x	[52] 4.2	c13	c13
24E	P-Charging-Function-Addresses	[52] 4.5	c20	c21	[52] 4.5	c20	c21
24F	P-Charging-Vector	[52] 4.6	c18	c19	[52] 4.6	c18	c19
24G	P-Early-Media	[109] 8	c34	c34	[109] 8	c34	c34
25	P-Media-Authorization	[31] 5.1	n/a	n/a	[31] 5.1	c11	c12
25A	P-Preferred-Identity	[34] 9.2	c7	c5	[34] 9.2	n/a	n/a
25B	P-Preferred-Service	[121] 4.2	c37	c36	[121] 4.2	n/a	n/a
25C	P-Profile-Key	[97] 5	n/a	n/a	[97] 5	n/a	n/a
25D	P-User-Database	[82] 4	n/a	n/a	[82] 4	n/a	n/a
25E	P-Visited-Network-ID	[52] 4.3	x (note 3)	x	[52] 4.3	c14	n/a
26	Priority	[26] 20.26	o	o	[26] 20.26	o	o
26A	Privacy	[33] 4.2	c9	c9	[33] 4.2	c9	c9
27	Proxy-Authorization	[26] 20.28	c6	c6	[26] 20.28	n/a	n/a
28	Proxy-Require	[26] 20.29	o (note 2)	o (note 2)	[26] 20.29	n/a	n/a
28A	Reason	[34A] 2	c8	c8	[34A] 2	c8	c8
29	Record-Route	[26] 20.30	n/a	n/a	[26] 20.30	m	m
30	Referred-By	[59] 3	c27	c27	[59] 3	c28	c28
31	Reject-Contact	[56B] 9.2	c24	c24	[56B] 9.2	c32	c32
31A	Replaces	[60] 6.1	c29	c29	[60] 6.1	c29	c29
31B	Reply-To	[26] 20.31	o	o	[26] 20.31	o	o
31B	Request-Disposition	[56B] 9.1	c24	c24	[56B] 9.1	c32	c32
32	Require	[26] 20.32	o	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

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
33B	Security-Verify	[48] 2.3.1	c23	c23	[48] 2.3.1	n/a	n/a
33C	Session-Expires	[58] 4	c25	c25	[58] 4	c25	c25
34	Subject	[26] 20.36	o	o	[26] 20.36	o	o
35	Supported	[26] 20.37	m	m	[26] 20.37	m	m
36	Timestamp	[26] 20.38	c10	c10	[26] 20.38	m	m
37	To	[26] 20.39	m	m	[26] 20.39	m	m
38	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
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 information.
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.3/1 AND A.4/25 THEN o ELSE n/a - - UE and private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c6: IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c7: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c8: IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.
c9: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c10: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.
c11: IF A.4/19 THEN m ELSE n/a - - SIP extensions for media authorization.
c12: IF A.3/1 THEN m ELSE n/a - - UE.
c13: IF A.4/32 THEN o ELSE n/a - - the P-Called-Party-ID extension.
c14: IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.
c15: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c16: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c17: IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c18: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c19: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c20: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c21: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c22: IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 4).
c23: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c24: IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.
c25: IF A.4/42 THEN m ELSE n/a - - the SIP session timer.
c26: IF A.4/42 THEN o ELSE n/a - - the SIP session timer.
c27: IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.
c28: IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.
c29: IF A.4/44 THEN m ELSE n/a - - the Session Initiation Protocol (SIP) "Replaces" header.
c30: IF A.4/45 THEN m ELSE n/a - - the Session Initiation Protocol (SIP) "Join" header.
c31: IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c32: IF A.4/40 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
c33: IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c34: IF A.4/66 THEN m ELSE n/a - - The SIP P-Early-Media private header extension for authorization of early media.
c36: IF A.3/1 AND A.4/74 THEN o ELSE n/a - - UE and identification of communication services in the session initiation protocol.
c37: IF A.4/74 THEN o ELSE n/a - - Identification of communication services in the session initiation protocol.
c38: IF A.4/74 THEN m ELSE n/a - - Identification of communication services in the session initiation protocol.
o.1: At least one of these shall be supported.

NOTE 1: RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.
NOTE 2: No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.
NOTE 3: The strength of this requirement in RFC 3455 [52] is SHOULD NOT, rather than MUST NOT.
NOTE 4: Support of this header in this method is dependent on the security mechanism and the security architecture which is implemented. Use of this header in this method is not appropriate to the security mechanism defined by 3GPP TS 33.203 [19].

Table A.47: Void

Prerequisite A.5/9 - - INVITE response

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

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	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.							

Prerequisite A.5/9 - - INVITE response for all remaining status-codes

Table A.49: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	c12	c12	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
1A	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
8[a]	Expires	[26] 20.19	o	o	[26] 20.19	o	o
9	From	[26] 20.20	m	m	[26] 20.20	m	m
9A	Geolocation	[89] 3.2	c14	c14	[89] 3.2	c14	c14
9B	History-Info	[66] 4.1	c13	c13	[66] 4.1	c13	c13
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
11	Organization	[26] 20.25	o	o	[26] 20.25	o	o
11A	P-Access-Network-Info	[52] 4.4	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	c11	c11
11D	P-Charging-Vector	[52] 4.6	c8	c9	[52] 4.6	c8	c9
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	Reply-To	[26] 20.31	o	o	[26] 20.31	o	o
11H	Require	[26] 20.32	m	m	[26] 20.32	m	m
11I	Server	[26] 20.35	o	o	[26] 20.35	o	o
11J	Reason	Annex ZB		c15	Annex ZB		c15
12	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
13	To	[26] 20.39	m	m	[26] 20.39	m	m
13A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
15	Warning	[26] 20.43	o (note)	o	[26] 20.43	o	o

c1: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c2: IF A.4/6 THEN m ELSE n/a - - timestamping of requests.
c3: IF A.4/25 THEN o ELSE n/a - - private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c4: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c5: IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c6: IF A.4/34 AND A.3/1 THEN m ELSE n/a - - the P-Access-Network-Info header extension and UE.
c7: IF A.4/34 AND (A.3/7A OR A.3/7D) THEN m ELSE n/a - - the P-Access-Network-Info header extension and AS acting as terminating UA or AS acting as third-party call controller.
c8: IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c9: IF A.4/36 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c10: IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c11: IF A.4/35 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c12: IF A.6/6 OR A.6/18 THEN m ELSE o - - 200 (OK), 405 (Method Not Allowed).
c13: IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c14: IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.
c15: IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.

NOTE: For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/101A - - Additional for 18x response

Table A.50: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Contact	[26] 20.10	o	m	[26] 20.10	m	m
5	P-Answer-State	[111]	c13	c13	[111]	c13	c13
5A	P-Early-Media	[109] 8	c14	c14	[109] 8	c14	c14
6	P-Media-Authorization	[31] 5.1	n/a	n/a	[31] 5.1	c11	c12
9	Rseq	[27] 7.1	c2	m	[27] 7.1	c3	m
c2:	IF A.4/14 THEN o ELSE n/a - - reliability of provisional responses in SIP.						
c3:	IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses in SIP.						
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 - - UE.						
c13:	IF A.4/65 THEN m ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular.						
c14:	IF A.4/66 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.						

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.51: 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	o	o	[26] 20.1	m	m
1A	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
1B	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
2	Allow-Events	[28] 7.2.2	c3	c3	[28] 7.2.2	c4	c4
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
7	P-Answer-State	[111]	c14	c14	[111]	c14	c14
8	P-Media-Authorization	[31] 5.1	n/a	n/a	[31] 5.1	c11	c12
9	Record-Route	[26] 20.30	m	m	[26] 20.30	m	m
10	Session-Expires	[58] 4	c13	c13	[58] 4	c13	c13
13	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.						
c2:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						
c3:	IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension.						
c4:	IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.						
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 - - UE.						
c13:	IF A.4/42 THEN m ELSE n/a - - the SIP session timer.						
c14:	IF A.4/65 THEN m ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular.						

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.51A: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

Table A.52: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Contact	[26] 20.10	o (note 1)	o	[26] 20.10	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/9 - - INVITE response

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

Table A.53: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
6	Proxy-Authenticate	[26] 20.27	c3	c3	[26] 20.27	c3	c3
13	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.						
c3:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 600 (Busy Everywhere), 603 (Decline) response

Table A.54: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
8	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.55: Void

Prerequisite A.5/9 - - INVITE response

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

Table A.56: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
6	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
11	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.4/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/9 - - INVITE response

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

Table A.57: Supported headers within the INVITE 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	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/9 - - INVITE response

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

Table A.58: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
10	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/9 - - INVITE response

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

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

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	x	x	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/28A - - Additional for 422 (Session Interval Too Small) response

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

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Min-SE	[58] 5	c1	c1	[58] 5	c1	c1
c1:	IF A.4/42 THEN o ELSE n/a - - the SIP session timer.						

Table A.59: Void

Table A.60: Void

Prerequisite A.5/9 - - INVITE response

Prerequisite: A.6/45 - - 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
8	Retry-After	[26] 20.33	o	o	[26] 20.33	o	m

Prerequisite A.5/9 - - INVITE response

Table A.62: Supported message bodies within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

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 status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	o	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
3A	Allow	[26] 20.5	o	o	[26] 20.5	m	m
4	Allow-Events	[28] 7.2.2	c27	c27	[28] 7.2.2	c1	c1
5	Authorization	[26] 20.7, [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	o	o	[26] 20.9	o	o
8	Contact	[26] 20.10	o	m	[26] 20.10	m	m
9	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
10	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
11	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
14	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	c3	c3	[26] 20.17	m	m
16	Expires	[26] 20.19	o	o	[26] 20.19	m	m
17	From	[26] 20.20	m	m	[26] 20.20	m	m
17A	Geolocation	[89] 3.2	c31	c31	[89] 3.2	c31	c31
17B	History-Info	[66] 4.1	c28	c28	[66] 4.1	c28	c28
18	Max-Forwards	[26] 20.22	m	m	[26] 20.22	n/a	n/a
19	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
20	Organization	[26] 20.25	o	o	[26] 20.25	o	o
20A	P-Access-Network-Info	[52] 4.4	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-User-Database	[82] 4	n/a	n/a	[82] 4	c30	c30
20E	P-Visited-Network-ID	[52] 4.3	x (note 2)	x	[52] 4.3	c10	c11
20FE	Path	[35] 4	c4	c5	[35] 4	m	c6
20GF	Privacy	[33] 4.2	c9	n/a	[33] 4.2	c9	n/a
21	Proxy-Authorization	[26] 20.28	c8	c8	[26] 20.28	n/a	n/a
22	Proxy-Require	[26] 20.29	o	o (note 1)	[26] 20.29	n/a	n/a
22A	Reason	[34A] 2	c23	c23	[34A] 2	c23	c23
22B	Referred-By	[59] 3	c25	c25	[59] 3	c26	c26
22C	Request-Disposition	[56B] 9.1	c24	c24	[56B] 9.1	n/a	n/a
23	Require	[26] 20.32	o	o	[26] 20.32	m	m
24	Route	[26] 20.34	o	n/a	[26] 20.34	n/a	n/a
24A	Security-Client	[48] 2.3.1	c19	c20	[48] 2.3.1	n/a	n/a
24B	Security-Verify	[48] 2.3.1	c20	c20	[48] 2.3.1	c21	n/a
25	Supported	[26] 20.37	o	c29	[26] 20.37	m	m
26	Timestamp	[26] 20.38	c7	c7	[26] 20.38	c7	c7
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
29	Via	[26] 20.42	m	m	[26] 20.42	m	m

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
c1:	IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.						
c2:	IF A.4/8 THEN m ELSE n/a - - authentication between UA and registrar.						
c3:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c4:	IF A.4/24 THEN o ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.						
c5:	IF A.4/24 THEN x ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.						
c6:	IF A.3/4 THEN m ELSE n/a. - - S-CCF.						
c7:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.						
c8:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.						
c9:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c10:	IF A.4/33 THEN o ELSE n/a - - the P-Visited-Network-ID extension.						
c11:	IF A.4/33 THEN m ELSE n/a - - the P-Visited-Network-ID extension.						
c12:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c13:	IF A.4/34 AND (A.3/1 OR A.3/4) THEN o ELSE n/a - - the P-Access-Network-Info header extension and UE or S-CCF.						
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-CCF or AS acting as terminating UA.						
c15:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c16:	IF A.4/36 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Vector header extension (including S-CCF as registrar).						
c17:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c18:	IF A.4/35 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension (including S-CCF as registrar).						
c19:	IF A.4/37 THEN o ELSE n/a - - security mechanism agreement for the session initiation protocol (note 3).						
c20:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						
c21:	IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar.						
c22:	IF A.3/4 THEN m ELSE n/a - - S-CCF.						
c23:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.						
c24:	IF A.4/40 THEN o ELSE n/a - - caller preferences for the session initiation protocol.						
c25:	IF A.4/43 THEN m ELSE n/a - - the SIP Referred-By mechanism.						
c26:	IF A.4/43 THEN o ELSE n/a - - the SIP Referred-By mechanism.						
c27:	IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension.						
c28:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						
c29:	IF A.3/1 THEN m ELSE o - - UE.						
c30:	IF A.4/48 THEN m ELSE n/a - - the P-User-Database private header extension.						
c31:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.						
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.						

Table A.120: Void

Table A.121: Void

Prerequisite A.5/19 - - REGISTER response

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

Table A.121A: 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	c1	c1	[26] 20.17	m	m
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						

Prerequisite A.5/19 - - REGISTER response for all status-codes

Table A.122: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
0A	Allow	[26] 20.5	c8	c8	[26] 20.5	m	m
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
1A	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
2	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
3	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
4	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
9	From	[26] 20.20	m	m	[26] 20.20	m	m
9A	Geolocation	[89] 3.2	c10	c10	[89] 3.2	c10	c10
9B	History-Info	[66] 4.1	c9	c9	[66] 4.1	c9	c9
10	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
11	Organization	[26] 20.25	o	o	[26] 20.25	o	o
11A	P-Access-Network-Info	[52] 4.4	c3	n/a	[52] 4.4	c3	n/a
11B	P-Charging-Function-Addresses	[52] 4.5	c6	c7	[52] 4.5	c6	c7
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	o	o	[26] 20.35	o	o
12	Timestamp	[26] 20.38	c2	c2	[26] 20.38	m	m
13	To	[26] 20.39	m	m	[26] 20.39	m	m
13A	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
15	Warning	[26] 20.43	o (note)	o	[26] 20.43	o	o

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).						
c3:	IF A.4/34 THEN o ELSE n/a - - the P-Access-Network-Info header extension.						
c4:	IF A.4/36 THEN o ELSE n/a - - the P-Charging-Vector header extension.						
c5:	IF A.4/36 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Vector header extension (including S-CCF as registrar).						
c6:	IF A.4/35 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.						
c7:	IF A.4/35 OR A.3/4 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension (including S-CCF as registrar).						
c8:	IF A.6/18 THEN m ELSE o - - 405 (Method Not Allowed).						
c9:	IF A.4/47 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						
c10:	IF A.4/60 THEN m ELSE n/a - - SIP location conveyance.						
NOTE:	For a 488 (Not Acceptable Here) response, RFC 3261 [26] gives the status of this header as SHOULD rather than OPTIONAL.						

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/102 - - Additional for 2xx response

Table A.123: 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	o		[26] 20.1	o	
1A	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
1B	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
2	Allow-Events	[28] 7.2.2	c12	c12	[28] 7.2.2	c13	c13
3	Authentication-Info	[26] 20.6	c6	c6	[26] 20.6	c7	c7
5	Contact	[26] 20.10	o	o	[26] 20.10	m	m
5A	P-Associated-URI	[52] 4.1	c8	c9	[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 ELSE n/a. - - S-CCF acting as registrar.						
c2:	IF A.3/4 OR A.3/1THEN m ELSE n/a. - - S-CCF or UE.						
c3:	IF A.4/24 THEN m ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.						
c4:	IF A.4/24 THEN o ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.						
c5:	IF A.4/28 THEN m ELSE n/a - - session initiation protocol extension header field for service route discovery during registration.						
c6:	IF A.4/8 THEN o ELSE n/a - - authentication between UA and registrar.						
c7:	IF A.4/8 THEN m ELSE n/a - - authentication between UA and registrar.						
c8:	IF A.4/2 AND A.4/31 THEN m ELSE n/a - - P-Associated-URI header extension and registrar.						
c9:	IF A.3/1 AND A.4/31 THEN m ELSE n/a - - P-Associated-URI header extension and S-CCF.						
c10:	IF A.4/31 THEN o ELSE n/a - - P-Associated-URI header extension.						
c11:	IF A.4/31 AND A.3/1 THEN m ELSE n/a - - P-Associated-URI header extension and UE.						
c12:	IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension.						
c13:	IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.						

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/103 OR A.6/104 OR A.6/105 OR A.6/106 - - Additional for 3xx – 6xx response

Table A.123A: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/103 OR A.6/35 - - Additional for 3xx or 485 (Ambiguous) response

Table A.124: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Contact	[26] 20.10	o (note)	o	[26] 20.10	m	m

Prerequisite A.5/19 - - REGISTER response

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

Table A.125: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Proxy-Authenticate	[26] 20.27	c1	x	[26] 20.27	c1	x
6	Security-Server	[48] 2	x	x	[48] 2	n/a	c2
10	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A. 4/8 THEN m ELSE n/a - - support of authentication between UA and registrar.						
c2:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Prerequisite A.5/19 - - REGISTER response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 503 (Service Unavailable), 600 (Busy Everywhere), 603 (Decline) response

Table A.126: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
6	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o

Table A.127: Void

Prerequisite A.5/19 - - REGISTER response

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

Table A.128: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
5	Proxy-Authenticate	[26] 20.27	c1	x	[26] 20.27	c1	x
9	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.4/8 THEN m ELSE n/a - - support of authentication between UA and registrar.						

Prerequisite A.5/19 - - REGISTER response

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

Table A.129: Supported headers within the REGISTER 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	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/19 - - REGISTER response

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

Table A.130: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
8	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/19 - - REGISTER response

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

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

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	c2	c2	[48] 2	c1	c1
c1:	IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						
c2:	IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar.						

Prerequisite A.5/19 - - REGISTER response

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

Table A.131: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
5	Min-Expires	[26] 20.23	m	m	[26] 20.23	m	m

Table A.132: Void

Table A.133: Void

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	x	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	c31
7	support of indication of TLS connections in the Record-Route header on the upstream side?	[26] 16.7	o	n/a
8	support of indication TLS connections in the Record-Route header on the downstream side?	[26] 16.7	o	n/a
8A	authentication between UA and proxy?	[26] 20.28, 22.3	o	x
9	insertion of date in requests and responses?	[26] 20.17	o	o
10	suppression or modification of alerting information data?	[26] 20.4	o	o
11	reading the contents of the Require header before proxying the request or response?	[26] 20.32	o	o
12	adding or modifying the contents of the Require header before proxying the REGISTER request or response	[26] 20.32	o	m
13	adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER?	[26] 20.32	o	o
14	being able to insert itself in the subsequent transactions in a dialog (record-routing)?	[26] 16.6	o	c2
15	the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing?	[26] 16.7	c3	c3
16	reading the contents of the Supported header before proxying the response?	[26] 20.37	o	o
17	reading the contents of the Unsupported header before proxying the 420 response to a REGISTER?	[26] 20.40	o	m
18	reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER?	[26] 20.40	o	o
19	the inclusion of the Error-Info header in 3xx - 6xx responses?	[26] 20.18	o	o
19A	reading the contents of the Organization header before proxying the request or response?	[26] 20.25	o	o
19B	adding or concatenating the Organization header before proxying the request or response?	[26] 20.25	o	o
19C	reading the contents of the Call-Info header before proxying the request or response?	[26] 20.25	o	o
19D	adding or concatenating the Call-Info header before proxying the request or response?	[26] 20.25	o	o
19E	delete Contact headers from 3xx responses prior to relaying the response?	[26] 20	o	o
	Extensions			
20	the SIP INFO method?	[25]	o	o
21	reliability of provisional responses in SIP?	[27]	o	i

Item	Does the implementation support	Reference	RFC status	Profile status
22	the REFER method?	[36]	o	o
23	integration of resource management and SIP?	[30] [64]	o	i
24	the SIP UPDATE method?	[29]	c4	i
26	SIP extensions for media authorization?	[31]	o	c7
27	SIP specific event notification	[28]	o	i
28	the use of NOTIFY to establish a dialog	[28] 4.2	o	n/a
29	Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts	[35]	o	c6
30	extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks	[34]	o	m
30A	act as first entity within the trust domain for asserted identity	[34]	c5	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]	o	m
31A	request of privacy by the inclusion of a Privacy header	[33]	n/a	n/a
31B	application of privacy based on the received Privacy header	[33]	c10	c12
31C	passing on of the Privacy header transparently	[33]	c10	c13
31D	application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the assistance of intermediaries are obscured?	[33] 5.1	x	x
31E	application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs?	[33] 5.2	n/a	n/a
31F	application of the privacy option "user" such that user level privacy functions are provided by the network?	[33] 5.3	n/a	n/a
31G	application of the privacy option "id" such that privacy of the network asserted identity is provided by the network?	[34] 7	c11	c12
31H	application of the privacy option "history" such that privacy of the History-Info header is provided by the network?	[66] 7.2	c34	c34
32	Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration	[38]	o	c30
33	a messaging mechanism for the Session Initiation Protocol (SIP)	[50]	o	m
34	Compressing the Session Initiation Protocol	[55]	o	c7
35	private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)?	[52]	o	m
36	the P-Associated-URI header extension?	[52] 4.1	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 for access network information?	[52] 4.4	c20	c21

Item	Does the implementation support	Reference	RFC status	Profile status
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]	o	c7
48	the Reason header field for the session initiation protocol	[34A]	o	o
49	an extension to the session initiation protocol for symmetric response routeing	[56A]	o	m
50	caller preferences for the session initiation protocol?	[56B]	c33	c33
50A	the proxy-directive within caller-preferences?	[56B] 9.1	o.4	o.4
50B	the cancel-directive within caller-preferences?	[56B] 9.1	o.4	o.4
50C	the fork-directive within caller-preferences?	[56B] 9.1	o.4	c32
50D	the recurse-directive within caller-preferences?	[56B] 9.1	o.4	o.4
50E	the parallel-directive within caller-preferences?	[56B] 9.1	o.4	c32
50F	the queue-directive within caller-preferences?	[56B] 9.1	o.4	o.4
51	an event state publication extension to the session initiation protocol?	[70]	o	m
52	SIP session timer?	[58]	o	o
53	the SIP Referred-By mechanism?	[59]	o	o
54	the Session Initiation Protocol (SIP) "Replaces" header?	[60]	o	o
55	the Session Initiation Protocol (SIP) "Join" header?	[61]	o	o
56	the caller capabilities?	[62]	o	o
57	an extension to the session initiation protocol for request history information?	[66]	o	o
58	Rejecting anonymous requests in the session initiation protocol?	[67]	o	o
59	session initiation protocol URIs for applications such as voicemail and interactive voice response	[68]	o	o
60	the P-User-Database private header extension?	[82]	o	o
61	Session initiation protocol's non-INVITE transactions?	[83]	m	m
62	a uniform resource name for services	[69]	n/a	c35
63	obtaining and using GRUUs in the Session Initiation Protocol (SIP)	[93]	o	c36
64	an extension to the session initiation protocol for request cpc information?	[95]	o	c37
65	the Stream Control Transmission Protocol (SCTP) as a Transport for the Session Initiation Protocol (SIP)?	[96]	o	o (note2)
66	the SIP P-Profle-Key private header extension?	[97]	o	c41
66A	making the first query to the database in order to populate the P-Profile-Key	[97]	c38	c39

Item	Does the implementation support	Reference	RFC status	Profile status
	header?			
66B	using the information in the P-Profile-Key header?	[97]	c38	c40
67	managing client initiated connections in SIP?	[92] 11	o	c42
69	multiple-recipient MESSAGE requests in the session initiation protocol	[104]	n/a	n/a
70	SIP location conveyance?	[89]	o	m
70A	addition or modification of location in a SIP method?	[89]	c44	c45
70B	passes on locations in SIP method without modification?	[89]	c44	c46
71	referring to multiple resources in the session initiation protocol?	[105]	n/a	n/a
72	conference establishment using request-contained lists in the session initiation protocol?	[106]	n/a	n/a
73	subscriptions to request-contained resource lists in the session initiation protocol?	[107]	n/a	n/a
74	dialstring parameter for the session initiation protocol uniform resource identifier?	[103]	o	n/a
75	the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular?	[111]	o	c60
76	the SIP P-Early-Media private header extension for authorization of early media?	[109] 8	o	c51
81	addressing an amplification vulnerability in session initiation protocol forking proxies?	[117]	c52	c52
82	the remote application identification of applying signalling compression to SIP	[79] 9.1	o	c7
83	a session initiation protocol media feature tag for MIME application sub-types?	[120]	o	c53
84	identification of communication services in the session initiation protocol?	[121]	o	c54
84A	act as authentication entity within the trust domain for asserted service?	[121]	c55	c56
85	XML Schema for PSTN?	[ANNEX ZB]	m	c61

Item	Does the implementation support	Reference	RFC status	Profile status
c1:	IF A.162/5 THEN o ELSE n/a - - stateful proxy behaviour.			
c2:	IF A.3/2 OR A.3/9A OR A.3/4 THEN m ELSE o - - P-CSCF, IBCF (THIG) or S-CCF.			
c3:	IF (A.162/7 AND NOT A.162/8) OR (NOT A.162/7 AND A.162/8) THEN m ELSE IF A.162/14 THEN o ELSE n/a - - TLS interworking with non-TLS else proxy insertion.			
c4:	IF A.162/23 THEN m ELSE o - - integration of resource management and SIP.			
c5:	IF A.162/30 THEN o ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.			
c6:	IF A.3/2 OR A.3/9A THEN m ELSE n/a - - P-CSCF or IBCF (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 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 - - S-CCF or AS acting as proxy and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks (note 1).			
c10:	IF A.162/31 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).			
c11:	IF A.162/31B THEN o ELSE x - - application of privacy based on the received Privacy header.			
c12:	IF A.162/31 AND A.3/4 THEN m ELSE n/a - - S-CCF.			
c13:	IF A.162/31 AND (A.3/2 OR A.3/3 OR A.3/7C OR A.3/9A) THEN m ELSE n/a - - P-CSCF or I-CSCF or AS acting as a SIP proxy or IBCF (THIG).			
c14:	IF A.162/35 THEN o.3 ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP).			
c15:	IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/9A) THEN m THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF or IBCF (THIG).			
c16:	IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/4 OR A.3/9A) 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-CCF or IBCF (THIG).			
c17:	IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/9A) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF or IBCF (THIG).			
c18:	IF A.162/38 THEN o ELSE n/a - - the P-Visited-Network-ID header extension.			
c19:	IF A.162/35 AND (A.3/2 OR A.3.3 OR A.3/4 OR A.3/7 THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF, I-CSCF, S-CCF, AS acting as a proxy.			
c20:	IF A.162/41 THEN o ELSE n/a - - the P-Access-Network-Info header extension.			
c21:	IF A.162/41 AND A.3/2 THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF.			
c22:	IF A.162/41 AND A.3/4 THEN m ELSE n/a - - the P-Access-Network-Info header extension and S-CCF.			
c23:	IF A.162/45 THEN o ELSE n/a - - the P-Charging-Vector header extension.			
c24:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.			
c25:	IF A.162/44 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.			
c26:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function Addresses header extension.			
c27:	IF A.3/2 OR A.3/4 THEN m ELSE x - - P-CSCF or S-CCF.			
c28:	IF A.3/2 OR A.3/4 OR A.3/6 then m ELSE o - - P-CSCF or S-CCF of MGCF.			
c29:	IF A.3/2 OR A.3/4 OR A.3/6 then o ELSE m - - P-CSCF or S-CCF of MGCF.			
c30:	IF A.3/2 o ELSE i - - P-CSCF.			
c31:	IF A.3/4 THEN m ELSE x - - S-CCF.			
c32:	IF A.3/4 THEN m ELSE o.4 - - S-CCF.			
c33:	IF A.162/50A OR A.162/50B OR A.162/50C OR A.162/50D OR A.162/50E OR A.162/50F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol.			
c34:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.			

Item	Does the implementation support	Reference	RFC status	Profile status
c35:	IF A.3/2 OR A.3/11 THEN m ELSE n/a - - P-CSCF, E-CSCF.			
c36:	IF A.3/4 THEN m ELSE n/a - - S-CCF.			
c37:	IF A.3/2 OR A.3/3 OR A.3/4 OR A.3.5 OR A.3/6 OR A.3/7 OR A.3/8 OR A.3/9A THEN o ELSE n/a - - cpc URI parameter.			
c38:	IF A.162/66 THEN o ELSE n/a - - the SIP P-Profile-Key private header.			
c39:	IF A.162/66 AND (A.3/3 OR A.3/9A) THEN m ELSE n/a - - the SIP P-Profile-Key private header, I-CSCF or IBCF (THIG).			
c40:	IF A.162/66 AND A.3/4 THEN m ELSE n/a - - the SIP P-Profile-Key private header, S-CCF.			
c41:	IF A.3/3 OR A.3/4 OR A.3/9A THEN o ELSE n/a - - I-CSCF or S-CCF or IBCF (THIG).			
c42:	IF A.3/2 OR A.3/4 THEN o ELSE n/a - - P-CSCF, S-CCF.			
c44:	IF A.162/70 THEN o.5 ELSE n/a - - SIP location conveyance.			
c45:	IF A.162/70 AND A.3/11 THEN m ELSE IF A.162/70 AND A.3/7C THEN o.6 ELSE n/a - - SIP location conveyance, E-CSCF, AS acting as a SIP proxy.			
c46:	IF A.162/70 AND A.3/2 OR A.3/3 OR A.3/5 OR A.3/10 THEN m ELSE IF A.162/70 AND A.3/7C THEN o.6 ELSE n/a - - SIP location conveyance, P-CSCF, I-CSCF, S-CCF, BGCF, additional routeing functionality.			
c51:	IF A.3/2 THEN m ELSE o - - P-CSCF.			
c52:	IF A.162/6 THEN m ELSE o - - forking of initial requests.			
c53:	IF A.3/4 THEN m ELSE n/a - - S-CCF.			
c54:	IF A.3/3 OR A.3/4 OR A.3/7 OR A.3/2 OR A.3/9A THEN m ELSE n/a - - I-CSCF, S-CCF, BGCF, P-CSCF. IBCF (THIG).			
c55:	IF A.162/84 THEN o ELSE n/a - - identification of communication services in the session initiation protocol.			
c56:	IF A.3/4 AND A.162/84 THEN m ELSE n/a - - S-CCF and identification of communication services in the session initiation protocol.			
c60:	IF A.3/2 OR A.3/3 OR A.3/4 THEN o ELSE n/a - - P=CSCF, I-CSCF, S-CCF.			
c61:	A.3/2 OR A.3/3 OR A.3/4 OR A.3/5 OR A.3/7C OR A.3/9A OR A.3/10 OR A.3/11 THEN o ELSE n/a - - P-CSCF, I-CSCF, S-CCF, BGCF, AS acting as proxy, IBCF (THIG), additional routeing functionality, E-CSCF.			
o.1:	It is mandatory to support at least one of these items.			
o.2:	It is mandatory to support at least one of these items.			
o.3:	It is mandatory to support at least one of these items.			
o.4	At least one of these capabilities is supported.			
o.5:	It is mandatory to support exactly one of these items.			
o.6:	It is mandatory to support exactly one of these items.			
NOTE 1:	An AS acting as a proxy may be outside the trust domain, and therefore not able to support the capability for that reason; in this case it is perfectly reasonable for the header to be passed on transparently, as specified in the PDU parts of the profile.			
NOTE 2:	Not applicable over Gm reference point (UE – P-CSCF).			

A.2.2.4.7 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
1A	Accept-Contact	[56B] 9.2	c34	c34	[56B] 9.2	c34	c35
2	Accept-Encoding	[26] 20.2	m	m	[26] 20.2	i	i
3	Accept-Language	[26] 20.3	m	m	[26] 20.3	i	i
4	Alert-Info	[26] 20.4	c2	c2	[26] 20.4	c3	c3
5	Allow	[26] 20.5	m	m	[26] 20.5	i	i
6	Allow-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
8	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
9	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
10	Call-Info	[26] 20.9	m	m	[26] 20.9	c12	c12
11	Contact	[26] 20.10	m	m	[26] 20.10	i	i
12	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	c6
13	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	c6
14	Content-Language	[26] 20.13	m	m	[26] 20.13	i	c6
15	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
16	Content-Type	[26] 20.15	m	m	[26] 20.15	i	c6
17	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
18	Date	[26] 20.17	m	m	[26] 20.17	c4	c4
19	Expires	[26] 20.19	m	m	[26] 20.19	i	i
20	From	[26] 20.20	m	m	[26] 20.20	m	m
20A	Geolocation	[89] 3.2	c47	c47	[89] 3.2	c48	c48
20B	History-Info	[66] 4.1	c43	c43	[66] 4.1	c43	c43
21	In-Reply-To	[26] 20.21	m	m	[26] 20.21	i	i
21A	Join	[61] 7.1	c41	c41	[61] 7.1	c42	c42
22	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
23	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	c6
23A	Min-SE	[58] 5	o	o	[58] 5	o	o
24	Organization	[26] 20.25	m	m	[26] 20.25	c5	c5
24A	P-Access-Network-Info	[52] 4.4	c28	c28	[52] 4.4	c29	c30
24B	P-Asserted-Identity	[34] 9.1	c15	c15	[34] 9.1	c16	c16
24C	P-Asserted-Service	[121] 4.1	c53	c53	[121] 4.1	c54	c54
24D	P-Called-Party-ID	[52] 4.2	c19	c19	[52] 4.2	c20	c21
24E	P-Charging-Function-Addresses	[52] 4.5	c26	c27	[52] 4.5	c26	c27
24F	P-Charging-Vector	[52] 4.6	c24	c24	[52] 4.6	c25	c25
24G	P-Early-Media	[109] 8	o	c50	[109] 8	o	c51
25	P-Media-Authorization	[31] 5.1	c9	x	[31] 5.1	n/a	n/a
25A	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c14	c14
25B	P-Preferred-Service	[121] 4.2	x	x	[121] 4.2	c52	c52
25B	P-Profile-Key	[97] 5	c45	c45	[97] 5	c46	c46
25C	P-User-Database	[82] 4	c44	c44	[82] 4	c44	c44
25D	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, [34] 4	m	m	[26] 20.29, [34] 4	m	m
28A	Reason	[34A] 2	c32	c32	[34A] 2	c33	c33
29	Record-Route	[26] 20.30	m	m	[26] 20.30	c11	c11
30	Referred-By	[59] 3	c37	c37	[59] 3	c38	c38
31	Reject-Contact	[56B] 9.2	c34	c34	[56B] 9.2	c34	c35
31A	Replaces	[60] 6.1	c39	c39	[60] 6.1	c40	c40
31B	Reply-To	[26] 20.31	m	m	[26] 20.31	i	i
31B	Request-Disposition	[56B] 9.1	c34	c34	[56B] 9.1	c34	c34
32	Require	[26] 20.32	m	m	[26] 20.32	c7	c7
33	Route	[26] 20.34	m	m	[26] 20.34	m	m
33A	Security-Client	[48] 2.3.1	x	x	[48] 2.3.1	c31	c31

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
33B	Security-Verify	[48] 2.3.1	x	x	[48] 2.3.1	c31	c31
33C	Session-Expires	[58] 4	c36	c36	[58] 4	c36	c36
34	Subject	[26] 20.36	m	m	[26] 20.36	i	i
35	Supported	[26] 20.37	m	m	[26] 20.37	c8	c8
36	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
37	To	[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 - - SIP specific event notification extension.
c2: IF A.162/10 THEN n/a ELSE m - - suppression or modification of alerting information data.
c3: IF A.162/10 THEN m ELSE i - - suppression or modification of alerting information data.
c4: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c5: IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c6: IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CCF.
c7: IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.
c8: IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.
c9: IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization.
c11: IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.
c12: IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c13: IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.
c14: IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c15: IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c16: IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.
c17: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c18: IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
c19: IF A.162/37 THEN m ELSE n/a - - the P-Called-Party-ID header extension.
c20: IF A.162/37 THEN i ELSE n/a - - the P-Called-Party-ID header extension.
c21: IF A.162/37 AND A.3/2 THEN m ELSE IF A.162/37 AND (A.3/3 OR A.3/9A) THEN i ELSE n/a - - the P-Called-Party-ID header extension and P-CSCF or (I-CSCF or IBCF (THIG)).
c22: IF A.162/38 THEN m ELSE n/a - - the P-Visited-Network-ID header extension.
c23: IF A.162/39 THEN m ELSE i - - reading, or deleting the P-Visited-Network-ID header before proxying the request or response.
c24: IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c25: IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.
c26: IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c27: IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
c28: IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c29: IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c30: IF A.162/43 OR (A.162/41 AND A.3/2) THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension (with or without P-CSCF).
c31: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c32: IF A.162/48 THEN m ELSE n/a - - the Reason header field for the session initiation protocol.
c33: IF A.162/48 THEN i ELSE n/a - - the Reason header field for the session initiation protocol.
c34: IF A.162/50 THEN m ELSE n/a - - caller preferences for the session initiation protocol.
c35: IF A.162/50 AND A.4/3 THEN m ELSE IF A.162/50 AND NOT A.4/3 THEN i ELSE n/a - - caller preferences for the session initiation protocol, and S-CCF.
c36: IF A.162/52 THEN m ELSE n/a - - the SIP session timer.
c37: IF A.162/53 THEN i ELSE n/a - - the SIP Referred-By mechanism.
c38: IF A.162/53 THEN m ELSE n/a - - the SIP Referred-By mechanism.

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
c39:	IF A.162/54 THEN m ELSE n/a - - the Session Initiation Protocol (SIP) "Replaces" header.						
c40:	IF A.162/54 THEN i ELSE n/a - - the Session Initiation Protocol (SIP) "Replaces" header.						
c41:	IF A.162/55 THEN m ELSE n/a - - the Session Initiation Protocol (SIP) "Join" header.						
c42:	IF A.162/55 THEN i ELSE n/a - - the Session Initiation Protocol (SIP) "Join" header.						
c43:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.						
c44:	IF A.162/60 THEN m ELSE n/a - - the P-User-Database private header extension.						
c45:	IF A.162/66A THEN m ELSE n/a - - making the first query to the database in order to populate the P-Profile-Key header.						
c46:	IF A.162/66B THEN m ELSE n/a - - using the information in the P-Profile-Key header.						
c47:	IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.						
c48:	IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.						
c50:	IF A.162/76 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.						
c51:	IF A.162/76 THEN (IF A.3/2 THEN m ELSE i) ELSE n/a - - P-CSCF, using the information in the P-Early-Media header.						
c52:	IF A.162/84A THEN m ELSE n/a - - act as authentication entity within the trust domain for asserted service.						
c53:	IF A.162/84 THEN m ELSE n/a - - identification of communication services in the session initiation protocol.						
c54:	IF A.162/84 OR A.162/30B THEN m ELSE i - - identification of communication services in the session initiation protocol or subsequent entity within trust network that can route outside the trust network.						
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 - - Additional for 100 (Trying) response

Table A.206: 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	m	m	[26] 20.8	m	m
2	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
3	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
4	Date	[26] 20.17	c1	c1	[26] 20.17	c2	c2
5	From	[26] 20.20	m	m	[26] 20.20	m	m
6	To	[26] 20.39	m	m	[26] 20.39	m	m
7	Via	[26] 20.42	m	m	[26] 20.42	m	m
c1:	IF (A.162/9 AND A.162/5) OR A.162/4 THEN m ELSE n/a - - stateful proxy behaviour that inserts date, or stateless proxies.						
c2:	IF A.162/4 THEN i ELSE m - - Stateless proxy passes on.						

Prerequisite A.163/9 - - INVITE response for all remaining status-codes

Table A.207: Supported headers within the INVITE 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	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
1A	Call-Info	[26] 20.9	m	m	[26] 20.9	c4	c4
2	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	c3
3	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	c3
4	Content-Language	[26] 20.13	m	m	[26] 20.13	i	c3
5	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
6	Content-Type	[26] 20.15	m	m	[26] 20.15	i	c3
7	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
8	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
8A	Expires	[26] 20.19	m	m	[26] 20.19	i	i
9	From	[26] 20.20	m	m	[26] 20.20	m	m
9A	History-Info	[66] 4.1	c17	c17	[66] 4.1	c17	c17
10	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	c3
11	Organization	[26] 20.25	m	m	[26] 20.25	c2	c2
11A	P-Access-Network-Info	[52] 4.4	c14	c14	[52] 4.4	c15	c15
11B	P-Asserted-Identity	[34] 9.1	c6	c6	[34] 9.1	c7	c7
11C	P-Charging-Function-Addresses	[52] 4.5	c12	c12	[52] 4.5	c13	c13
11D	P-Charging-Vector	[52] 4.6	c10	c10	[52] 4.6	c11	c11
11E	P-Preferred-Identity	[34] 9.2	x	x	[34] 9.2	c5	n/a
11F	Privacy	[33] 4.2	c8	c8	[33] 4.2	c9	c9
11G	Reply-To	[26] 20.31	m	m	[26] 20.31	i	i
11H	Require	[26] 20.32	m	m	[26] 20.32	c16	c16
11I	Server	[26] 20.35	m	m	[26] 20.35	i	i
11J	Reason	Annex ZB		c20	Annex ZB		c20
12	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
13	To	[26] 20.39	m	m	[26] 20.39	m	m
13A	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
14	Via	[26] 20.42	m	m	[26] 20.42	m	m
15	Warning	[26] 20.43	m	m	[26] 20.43	i	i

c1:	IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c2:	IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c3:	IF A.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CCF.
c4:	IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c5:	IF A.162/30A THEN m ELSE n/a - - act as first entity within the trust domain for asserted identity.
c6:	IF A.162/30 THEN m ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c7:	IF A.162/30A or A.162/30B THEN m ELSE i - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks or subsequent entity within trust network that can route outside the trust network.
c8:	IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c9:	IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.
c10:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c11:	IF A.162/46 THEN m ELSE IF A.162/45 THEN i ELSE n/a - - adding, deleting, reading or modifying the P-Charging-Vector header before proxying the request or response or the P-Charging-Vector header extension.
c12:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function-Addresses header extension.
c13:	IF A.162/44A THEN m ELSE IF A.162/44 THEN i ELSE n/a - - adding, deleting or reading the P-Charging-Function-Addresses header before proxying the request or response, or the P-Charging-Function-Addresses header extension.
c14:	IF A.162/43 THEN x ELSE IF A.162/41 THEN m ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c15:	IF A.162/43 THEN m ELSE IF A.162/41 THEN i ELSE n/a - - act as subsequent entity within trust network for access network information that can route outside the trust network, the P-Access-Network-Info header extension.
c16:	IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.
c17:	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c18:	IF A.162/70 THEN m ELSE n/a - - SIP location conveyance.
c19:	IF A.162/70A THEN m ELSE IF A.162/70B THEN i ELSE n/a - - addition or modification of location in a SIP method, passes on locations in SIP method without modification.
c20:	IF A.4/38 THEN o ELSE n/a - - the Reason header field for the session initiation protocol.

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/101 A - - Additional for 180 response

Table A.208: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Contact	[26] 20.10	m	m	[26] 20.10	i	i
5	P-Answer-State	[111]	c13	c13	[111]	c14	c14
5A	P-Early-Media	[109] 8	o	c11	[109] 8	o	c12
6	P-Media-Authorization	[31] 5.1	c9	x	[31] 5.1	n/a	n/a
9	Rseq	[27] 7.1	m	m	[27] 7.1	i	i
11	Supported	[26] 20.37	m	m	[26] 20.37	i	i

c9:	IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization.
c11:	IF A.162/76 THEN m ELSE n/a - - the SIP P-Early-Media private header extension for authorization of early media.
c12:	IF A.162/76 THEN (IF A.3/2 THEN m ELSE i) ELSE n/a - - P-CSCF, using the information in the P-Early-Media header.
c13:	IF A.162/75 THEN m ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular.
c14:	IF A.162/75 THEN i ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular.

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/102 - - Additional for 2xx response

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	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-Events	[28] 7.2.2	m	m	[28] 7.2.2	c1	c1
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
7	P-Answer-State	[111]	c13	c13	[111]	c14	c14
8	P-Media-Authorization	[31] 5.1	c9	x	[31] 5.1	n/a	n/a
9	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
10	Session-Expires	[58] 4	c11	c11	[58] 4	c11	c11
13	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c1:	IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.						
c3:	IF A.162/14 THEN m ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.						
c9:	IF A.162/26 THEN m ELSE n/a - - SIP extensions for media authorization.						
c11:	IF A.162/52 THEN m ELSE n/a - - the SIP session timer.						
c13:	IF A.162/75 THEN m ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular.						
c14:	IF A.162/75 THEN i ELSE n/a - - the P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular.						

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/103 OR A.164/104 OR A.164/105 OR A.164/106 - - Additional for 3xx – 6xx response

Table A.209A: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/103 OR A.164/35 - - Additional for 3xx or 485 (Ambiguous) response

Table A.210: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
4	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1
c1:	IF A.162/19E THEN m ELSE i - - deleting Contact headers.						

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/14 - - Additional for 401 (Unauthorized) response

Table A.211: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
6	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
15	WWW-Authenticate	[26] 20.44	o		[26] 20.44	o	

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/50 OR A.164/51 - - Additional for 404 (Not Found), 413 (Request Entity Too Large), 480(Temporarily not available), 486 (Busy Here), 500 (Internal Server Error), 600 (Busy Everywhere), 603 (Decline) response

Table A.212: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
8	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
12	Via	[26] 20.42	m	m	[26] 20.42	m	m

Table A.213: Void

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/20 - - Additional for 407 (Proxy Authentication Required) response

Table A.214: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
6	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
11	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/25 - - Additional for 415 (Unsupported Media Type) response

Table A.215: Supported 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	i	i
2	Accept-Encoding	[26] 20.2	m	m	[26] 20.2	i	i
3	Accept-Language	[26] 20.3	m	m	[26] 20.3	i	i

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/27 - - Additional for 420 (Bad Extension) response

Table A.216: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
10	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3
c3:	IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER.						

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/28 OR A.164/41A - - Additional for 421 (Extension Required), 494 (Security Agreement Required) response

Table A.216A: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
3	Security-Server	[48] 2	c1	c1	[48] 2	n/a	n/a
c1:	IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.						

Prerequisite A.16/9 - - INVITE response

Prerequisite: A.164/28A - - Additional for 422 (Session Interval Too Small) response

Table A.216B: Supported headers within the INVITE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Min-SE	[58] 5	c1	c1	[58] 5	c1	c1
c1:	IF A.162/52 THEN m ELSE n/a - - the SIP session timer.						

Table A.217: Void

Table A.217A: Void

Prerequisite A.163/9 - - INVITE response

Prerequisite: A.164/45 - - 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
8	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i

Table A.218: Void

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] [64]	o	m
23	grouping of media lines	[53]	c3	c3
24	mapping of media streams to resource reservation flows	[54]	o	c1
25	SDP Bandwidth Modifiers for RTCP Bandwidth	[56]	o	o (NOTE)
26	TCP-based media transport in the session description protocol	[83]	o	c2
27	interactive connectivity establishment?	[99]	o	c4
28	session description protocol format for binary floor control protocol streams?	[108]	o	o
c1:	IF A.3/1 THEN ~~m~~o.1 ELSE n/a - - UE role.			
c2:	IF A.3/1 OR A.3/6 OR A.3/7 THEN o ELSE n/a - - UE, MGCF, AS.			
c3:	IF A.317/24 THEN m ELSE o - - mapping of media streams to resource reservation flows.			
c4	IF A.3/9B THEN m ELSE IF A.3/1 OR A.3/6 THEN o ELSE n/a - - IBCF, UE, MGCF.			
o.1:	The procedure is mandatory in case if there are access specific procedures which the UE is using.			
NOTE:	For "video" and "audio" media types that utilize RTP/RTCP, f the RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556 [56], then, it shall be specified. For other media types, it may be specified.			

Annex B

B.2 GPRS aspects when connected to the IM CN subsystem

For the purpose of the present document annex B of [1] applies.

Annex C UICC and USIM Aspects for access to the IM CN subsystem

For the purpose of the present document annex C of [1] applies, except for the addition of clause C.4.

C.4 Provisioning of ~~IMS~~ parameters for UEs without ISIM or USIM

In case the UE contains neither a USIM application nor a ISIM application, the following IMS parameters are assumed to be available to the UE:

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

These parameters may not necessarily reside in a UICC.

Annex D IP-Connectivity Access Network specific concepts when using I-WLAN to access IM CN subsystem

For the purpose of the present document annex D of [1] applies.

Annex E IP-Connectivity Access Network specific concepts when using xDSL to access IM CN subsystem

For the purpose of the present document annex E of [1] applies.

Annex F

Annex F applies with the exception that all occurrences of "IMS Access Gateway" and IMS Access Gateway over the Iq interface" are replaced with "transport functions".

For the purpose of this document annex F of [1] applies with the addition of clause F.4A.

F.4A NAT traversal for media

To keep NAT bindings and firewall pinholes open with uni-directional RTP traffic and enable the C-BGF to perform address latching, the UE shall send keep alive messages for each media stream. These messages shall be sent regardless of whether the media stream is currently inactive, send only, recvonly or sendrecv. It is recommended that the keepalive message be an empty (no payload) RTP packet with a payload type of 20 as long as the other end has not negotiated the use of this value. If this value has already been negotiated, then some other unused static payload type from Table 5 of RFC 3551 [89] shall be used.

F.4.1 Introduction

Subclause F.4.1 applies with the following modification to the first paragraph.

Modify the first paragraph as follows:

The procedures defined in subclause F.2 and F.3 remain unchanged except as noted below when ~~This subclause describes the SIP procedures for~~ supporting hosted NAT scenarios in case UDP encapsulated IPsec is not employed. In these scenarios the procedures for NAT traversal must take into account that all SIP requests and responses are not protected by an IPsec security association.

F.4.2 Registration

The procedures described in subclause F.4.2 apply with the following modifications.

When the P-CSCF receives a REGISTER request from the UE, the P-CSCF shall behave as of subclause F.4.2 with the addition of sub-item 6a).

The P-CSCF shall:

6a) If a P-CSCF registration timer is running, the P-CSCF may decide not to forward the REGISTER request if received half of the time before expiry of the S-CCF registration timer, unless the request is intended to update its capabilities according to RFC 3840 [62] or to modify the ICSI values or IARI values that the UE intends to use in the g.ims.app_ref feature tag. In such cases it shall build a 200 OK response, based on the contents of the 200 OK response to the previous REGISTER request and forward this response to the UE.

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall behave as of clause 5.2.2 with the addition of item 10:

10) Modify the value of the Expires header field and/or Expires parameter in the Contact header according to the transport protocol. In order to minimize the number of REGISTER requests to the S-CCF, it may also start a P-CSCF registration timer with a value of 600 seconds if the value received from the S-CCF was for greater than 1200 seconds, or to half of the time otherwise.

NOTE 1: The selected value should be smaller than twice the value of the NAT timeout for the transport protocol. For UDP, many NATs have a timeout as low as 30 seconds. Issues such as battery consumption might motivate longer NAT timeout values. .

NOTE 2: If outbound keep alive messages (See annex K) are received before the REGISTER message, this procedure is not required,

Annex G

Annex G applies with the exception that all occurrences of "IMS Access Gateway" and IMS Access Gateway over the Iq interface" are replaced with "transport functions".

Annex J CPC parameter definition

J.1 Introduction

This annex defines the use of the "CPC" URI parameter for use within SIP URI and Tel URI in the P-Asserted ID in the initial INVITE.

Editor's note: This annex is based on draft-mahy-iptel-cpc-04.txt and can be removed when the internet draft becomes an RFC and the usage of the CPC is allowed for SIP URI. If this solution does not become an RFC, this parameter will be documented in the present document.

The Calling Party's Category is represented as a tel URI or SIP URI parameter in a SIP request. The ABNF syntax is as follows:

```
cpc = cpc-tag "=" cpc-value
cpc-tag = "cpc"
cpc-value
= "ordinary" / "test" / "operator" /
"payphone" / "priority" / "data" /
"cellular" / "cellular-roaming" / ”ieps” / "unknown" /

genvalue
genvalue = 1*(alphanum / "-" / "." )
```

The Accept- Language header shall be used to express the language of the operator.

The semantics of these Calling Party's Category values are described below:

ordinary: The caller has been identified, and has no special features.

test: This is a test call that has been originated as part of a maintenance procedure.

operator: The call was generated by an operator position.

payphone: The calling station is a payphone.

priority: Calling subscriber with priority.

data: Data call (voice band data).

cellular: The calling station is a radio-telephone operating in its home network.

cellular-roaming: The calling station is a radio-telephone roaming in another network

ieps: This call is an ieps call

unknown: The CPC could not be ascertained.

NOTE 1: The choice of CPC values and their use are up to the Service Provider. CPC values can be exchanged across networks if specified in a bilateral agreement between the service providers.

NOTE 2: Additional national/regional CPC values may exist (e.g. prison, police, hotel, hospital, …)

J.2 Trust domain

Entities in the IM CN subsystem shall restrict CPC tel URI or SIP URI parameter to specific domains that are trusted and support the CPC parameter. Therefore for the purpose of the CPC parameter within this specification, a trust domain also applies. This trust domain is identical to that of the P-Asserted-Identity. If the communication is to be passed to an untrusted network or a network not supporting the CPC the CPC parameter shall be removed.

SIP functional entities within the trust domain will need to take action on the removal of the CPC parameter when the SIP signalling crosses the boundary of the trust domain.

J.9A Procedures at the S-CCF at the terminating network

The S-CCF at the terminating network shall delete any CPC parameter in each initial request for a dialog or a request for a standalone transaction in the tel URI or SIP URI of the P-Asserted-Identity before forwarding the request to the terminating user.

Add annex L

Annex L (normative): SIP Digest

Editor's Note: It is FFS whether the SIP digest and TLS procedures will be documented as shown here in annex-L, or will be organized in some other manner within this specification (for example, integrated with the procedures in the main body of this specification). Therefore, this annex can be regarded as a temporary place-holder for this material.

L.1 Scope

This annex describes the procedures to support SIP digest as an additional authentication mechanism, and to support TLS as an additional signalling security mechanism between the UE and P-CSCF. SIP digest is optional to implement. When SIP digest is supported, TLS can be used as an optional security mechanism. A UE, P-CSCF, or S-CCF that implements SIP digest shall support the requirements specified in subclause L.2. A UE or P-CSCF that implements TLS shall support the requirements specified in subclause L.3.

L.2 SIP digest

L.2.1 Procedures at the UE

L.2.1.1 General

A UE that implements SIP digest shall support the procedures specified in subclause 5.1, except as noted in the sub-clauses of this section. When performing the procedures of this annex and the procedures in subclause 5.1, the UE shall not apply procedures related to IPsec. These procedures are distinguished by the use of the term "security association".

When using SIP digest without TLS, the UE shall populate the Contact header with the port value of an unprotected port where the UE expects to receive requests from the P-CSCF.

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

L.2.1.2 Registration

L.2.1.2.1 Initial REGISTER

When performing SIP digest, the procedures of subclause 5.1.1.2 apply with the following differences.

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

For SIP digest, if the UE is configured not to use TLS, the UE shall not establish a TLS session toward the P-CSCF.

L.2.1.2.2 Subscription to the registration-state event package

When performing SIP digest, the procedures of subclause 5.1.1.3 apply with the following differences.

When using SIP digest without TLS, the UE shall populate the Contact header of the SUBSCRIBE request with the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests.

L.2.1.2.3 User-initiated reregistration and registration of an additional public user identity

When performing SIP digest, the procedures of subclause 5.1.1.4 apply with the following differences.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the nonce directive with the empty value.

When using SIP digest without TLS, the UE shall populate the Contact header of the REGISTER request with the port value of an unprotected port where the UE expects to receive subsequent requests.

When using SIP digest without TLS, the UE shall populate the Via header of the REGISTER request with the port value of an unprotected port where the UE expects to receive responses to the request.

L.2.1.2.4 General Authentication

When performing SIP digest, the procedures in subclause 5.1.1.5.1 apply with the following differences.

On receiving a 401 (Unauthorized) response to the REGISTER request, and where the algorithm parameter is MD5, the UE shall extract the digest-challenge parameters as indicated in RFC 2617 [21] from the WWW-Authenticate header. The UE shall calculate digest-response parameters as indicated in RFC 2617 [21]. The UE shall send another REGISTER request containing an Authorization header containing a challenge response. If SIP digest is used without TLS, the UE shall not include RFC 3329 [48] headers with this REGISTER.

On receiving the 200 (OK) response for the REGISTER request, if the algorithm parameter in the Authentication-Info header is MD5, the UE shall authenticate the S-CCF using the "response-auth" directive in the Authentication-Info header as described in RFC 2617 [21].

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

L.2.1.2.5 User-initiated deregistration

When performing SIP digest, the procedures in subclause 5.1.1.6 apply with the following differences.

On sending a REGISTER request, the UE shall populate the nonce directive with the empty value.

When using SIP digest without TLS, the UE shall populate the Contact header of the REGISTER request with the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests.

When using SIP digest without TLS, the UE shall populate the Via header of the REGISTER request with the port value of an unprotected port where the UE expects to receive responses to the request.

L.2.1.3 Generic procedures applicable to all methods excluding the REGISTER method

When performing SIP digest, the procedures in subclause 5.1.2A and subclause 5.1.3 apply with the following differences.

When using SIP digest without TLS, if the UE does not support GRUU the UE shall populate the Contact header of the request with the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests.

When using SIP digest without TLS, the UE shall populate the Via header of the request with the port value of an unprotected port where the UE expects to receive responses to the request.

Upon receiving a 407 (Proxy Authentication Required) response to an initial request, the originating UE shall:

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

L.2.2 Procedures at the P-CSCF

L.2.2.1 General

A P-CSCF that implements SIP digest with or without TLS shall support the procedures specified in subclause 5.2, except as noted in the subclauses of this subclause. When performing the procedures of this annex and the procedures in subclause 5.2, the P-CSCF shall not apply procedures related to IPsec. These procedures are distinguished by the use of the term "security association".

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

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

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

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

If SIP digest is used without TLS, the P-CSCF shall discard any SIP messages received outside of the registration and authentication procedures that do not map to an existing IP association as defined in subclause L.2.2.2.

L.2.2.2 Registration

When performing SIP digest, the procedures in subclause 5.2.2 apply with the following differences.

When not applying TLS, the P-CSCF shall not include RFC 3329 [48] headers in registration messages towards the UE.

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

1) replacing step 4, if SIP digest is used without TLS, the P-CSCF shall not include the integrity-protected parameter.

When the P-CSCF receives a 200 (OK) response to a REGISTER request and the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

- in addition to the procedures in step 3, create an IP association by storing and associating the UE's packet source IP address along with the "sent-by" parameter of the Via header, cf. RFC 3261 [26], of the REGISTER message with the private user identity and all the successfully registered public user identities related to that private user identity. If draft-ietf-sip-outbound [92] is used then the P-CSCF shall also include the UE's packet source port of the REGISTER message as part of the IP association; and

- replacing step 9: if SIP digest is used without TLS, send the 200 (OK) response to the UE unprotected as defined in clause 4 of RFC 3581 [56A];

L.2.2.3 Requests initiated by the UE

When performing SIP digest, the procedures in subclause 5.2.6.3 apply with the following differences.

When the P-CSCF receives from the UE an initial request for a dialog or a request for a standalone transaction, and the request contains a P-Preferred-Identity header that does not match one of the registered public user identities mapped to the IP association, 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 than one default public user identity available, the P-CSCF shall randomly select one of them.

When the P-CSCF receives any 1xx or 2xx response to an initial request for a dialog, the P-CSCF shall:

- if SIP digest is used without TLS, in the response rewrite its own Record Route entry to its own SIP URI that contains an unprotected server port number where the P-CSCF expects subsequent requests from the UE.

L.2.2.4 Requests terminated by the UE

When performing SIP digest, the procedures in subclause 5.2.6.4 apply with the following differences.

When the P-CSCF receives, destined for the UE, an initial request for a dialog or a target refresh request for a dialog, and SIP digest is used without TLS, prior to forwarding the request, the P-CSCF shall:

- when adding its own SIP URI to the top of the list of Record-Route headers and saving the list, build the P-CSCF URI in a format that contains an unprotected server port number where the P-CSCF expects subsequent requests from the UE; and

- when adding its own address to the top of the received list of Via headers and saving the list, build the P-CSCF Via header entry in a format that contains an unprotected server port number where the P-CSCF expects responses to the current request from the UE.

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), or a response to this request and SIP digest is used without TLS, prior to forwarding the request, the P-CSCF shall:

- when adding its own address to the top of the received list of Via headers and saving the list, build the P-CSCF Via header entry in a format that contains an unprotected server port number where the P-CSCF expects responses to the current request from the UE.

L.2.2.5 General emergency services

When performing SIP digest procedures without TLS, the procedures in subclause 5.2.10.1 apply with the following differences.

NOTE: If only emergency setup from registered users is allowed, a request from an unregistered user is ignored since it is received outside of the IP association.

L.2.3 Procedures at the S-CCF

L.2.3.1 Initial registration and user-initiated reregistration

L.2.3.1.1 Unprotected REGISTER

When performing SIP digest, the procedures in subclause 5.4.1.2.1 apply with the following differences.

If the S-CCF receives a REGISTER request with a non-empty response parameter in the Authorization header, the S-CCF shall follow the protected REGISTER procedures as described in subclause 5.4.1.2.2.

NOTE: When SIP digest is used without TLS, the "integrity-protected" parameter can not be used to differentiate between an initial REGISTER or a protected REGISTER.

Upon receipt of a REGISTER request without an "integrity-protected" parameter or an "integrity-protected" parameter with the value "tls-yes", which is not for an already registered public user identity linked to the same private user identity, the S-CCF shall:

1) in Step 5, challenge the user by generating a 401 (Unauthorized) response for the received REGISTER request, including a WWW-Authenticate header as defined in RFC 2617 [21], which transports:

   - a protection domain in the realm field;

   - a domain field;

   - a nonce field;

   - an algorithm field; if the algorithm value is not provided in the authentication vector, it shall have the value "MD5"; and

   - a qop field; if the qop value is not provided in the authentication vector, it shall contain the value "auth".

NOTE: This specification does not make any assumption on which network entity generates the nonce.

L.2.3.1.2 Protected REGISTER

When performing SIP digest, the procedures in subclause 5.4.1.2.2 apply with the following differences.

Upon receipt of a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "tls-yes", or for SIP digest authentication without TLS, with a non-empty response parameter in the Authorization header, the S-CCF 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 a timer reg-await-auth is running for this user the S-CCF shall:

1) in Step 3, in the case the algorithm is MD5, check the following additional fields:

   - a realm field matching the realm field in the authentication challenge;

   - nonce field matching the nonce field in the authentication challenge;

   - a digest-uri matching the SIP Request URI;

   - a cnonce field; and

   - a nonce-count field.

   The S-CCF shall only proceed with the following steps in this paragraph if the authentication challenge response was included:

2) in Step 4, check whether the received authentication challenge response and the expected authentication challenge response match. The expected response is calculated by the S-CCF as described in RFC 2617 [21] using the H(A1) value provided by the HSS;

When creating a 200 (OK) for the REGISTER request, the S-CCF shall store the nonce-count value in the received REGISTER request and include an Authentication-Info header containing the fields described in RFC 2617 [21] as follows:

- a nextnonce field if the S-CCF requires a new nonce for subsequent authentication responses from the UE;

- a message-qop field matching the qop in Authorization header sent by the UE;

- a response-auth field with a response-digest calculated as described in RFC 2617 [21];

- a cnonce field matching the cnonce in the Authorization header sent by the UE; and

- a nonce-count field matching the nonce-count in the Authorization header sent by the UE.

L.2.3.1.3 Abnormal cases

When performing SIP digest, the procedures in subclause 5.4.1.2.3 apply with the following differences.

In the case that the REGISTER request, that contains the authentication challenge response from the UE does not match with the expected REGISTER request (e.g. wrong Call-Id or authentication challenge response) and the request has the "integrity-protected" parameter in the Authorization header set to "tls-yes" or contains no "integrity-protected" parameter, the S-CCF shall do one of the following:

- send a 403 (Forbidden) response to the UE. The S CSCF shall consider this authentication attempt as failed. The S-CCF shall not update the registration state of the subscriber; or

- rechallenge the user by issuing a 401 (Unauthorized) response including a challenge as per procedures described in subclause 5.4.1.2.1 starting at step 6).

NOTE: If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request from the UE contains an invalid nonce with a valid challenge response for that nonce (indicating that the client knows the correct username/password), or when the nonce-count value sent by the UE is not the expected value, the S-CCF shall:

- send a 401 (Unauthorized) response to initiate a further authentication attempt with a fresh nonce and the stale parameter set to true.

L.2.3.2 User-initiated deregistration

When performing SIP digest, the procedures in subclause 5.4.1.4 apply with the following differences.

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

- check whether the "integrity-protected" parameter in the Authorization header field set to "yes" or "tls-yes", indicating that the REGISTER request was received integrity protected. If the "integrity-protected" parameter is not present the S-CCF shall ensure authentication is performed as described in subclause 5.4.1.2.1 (and consequently subclause 5.4.1.2.2) if local policy requires. The S-CCF shall only proceed with the following steps if the "integrity-protected" parameter is set to "yes", "tls-yes", or the required authentication is successfully performed if required by local policy.

L.2.3.3 General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CCF

When performing SIP digest, the procedures in subclause 5.4.3 apply with the following differences.

When the S-CCF receives from the served user an initial request for a dialog or a request for a standalone transaction, the S-CCF may perform the steps in subclause L.2.3.4 to challenge the request based on local policy.

L.2.3.4 General authentication procedures for all SIP request methods initiated by the UE excluding REGISTER

L.2.3.4.1 General

When the S-CCF receives from the UE a request (excluding REGISTER), the S-CCF may perform the following steps if authentication of SIP request methods initiated by the UE excluding REGISTER is desired:

1) The S-CCF shall identify the user by the public user identity as received in the P-Asserted-Identity header.

2) If the public user identity does not match one of the registered public user identities, the S-CCF may reject the request with a 400 (Bad Request) response or silently discard the request.

3) If the request does not contain a Proxy-Authorization header or the Proxy-Authorization header does not contain a digest response, the S-CCF shall:

   a) challenge the user by generating a 407 (Proxy Authentication Required) response for the received request, including a Proxy-Authenticate header as defined in RFC 2617 [21], which includes:

      - a protection domain in the realm field;

      - a domain field;

      - a nonce field;

      - an algorithm field; if the algorithm value is not provided in the authentication vector, it shall have the value "MD5"; and

      - a qop field; if the qop value is not provided in the authentication vector, it shall have the value "auth".

   Editor's Note: It is FFS which entity generates the nonce.

   b) send the so generated 407 (Proxy Authentication Required) response towards the UE; and

   c) retain the nonce and initialize the corresponding nonce count to a value of 1.

4) If the request contains a Proxy-Authorization header, the S-CCF shall:

   a) check whether the Proxy-Authorization header contains:

      - the private user identity of the user in the username field;

- an algorithm field which matches the algorithm field in the authentication challenge (i.e. MD5);
- a response field with the authentication challenge response;
- a realm field matching the realm field in the authentication challenge;
- nonce field matching the expected nonce from either a recent authentication challenge or a more recent nextnonce sent in an Authentication-Info header;
- a digest-uri matching the SIP Request URI;
- a cnonce field; and
- a nonce-count field with a value that equals the nonce-count expected by the S-CCF. The S-CCF may choose to accept a nonce-count which is greater than the expected nonce-count only if the S-CCF uses this nonce-count once authentication is successful (and increments it for any subsequent authentication responses).

If any of the above checks do not succeed, the S-CCF shall proceed as described in subclause L.2.3.4.2, and skip the remainder of this procedure.

b) check whether the received authentication challenge response and the expected authentication challenge response match. The S-CCF shall compute the expected digest response as described in RFC 2617 [21] using the H(A1) value contained within the authentication vector, and other digest parameters (i.e. nonce, cnonce, nonce-count, qop).

In the case where the digest response does not match the expected digest response calculated by the S-CCF, the S-CCF shall consider the authentication attempt as failed and do one of the following:

1) rechallenge the user by issuing a 407 (Proxy Authentication Required) response including a challenge as per procedures described in this subclause; or
2) reject the request by issuing a 403 (Forbidden) response; or
3) reject the request without sending a response.

In the case where the digest response matches the expected digest response calculated by the S-CCF, the S-CCF shall consider the identity of the user verified and the request authenticated.

L.2.3.4.2 Abnormal cases

In the case that SIP digest is used and the request from the UE contains an invalid nonce with a valid challenge response for that nonce (indicating that the client knows the correct username/password), or when the nonce-count value sent by the UE is not the expected value, or when the Authorization header does not include the correct parameters, the S-CCF shall:

- send a 407 (Proxy Authentication Required) response to initiate a further authentication attempt with a fresh nonce and the stale parameter set to true.

Annex ZA (informative):

ZA.1 Void

ZA.2 Void

ZA.3 Void

ZA.4 Void

ZA.5 Void

ZA.6 Void

ZA.7 Void

ZA.8 Void

ZA.9 Void

ZA.9A Void

ZA.10 Void

ZA.11 Extensions needed in table A.162 of ES 283 003

Table A.162: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
XX	an extension to the session initiation protocol for request cpc information?	[xx]	o (note)	cxx
cxx	A.3/2 OR A.3/3 OR A.3/4 OR A.3.5 OR A.3/6 OR A.3/7 OR A.3/8 THEN o ELSE n/a - - cpc URI parameter			
NOTE:	It has to be clarified within the draft that the cpc value belongs to the trust domain and shall not be populated by UE's			

Annex ZB (informative): Procedures

For providing services and PSTN/ISDN interoperability it MUST be possible to include a Q.850 Cause value in Reason header field of a response.

The Reason Header is defined within RFC 3326 [34A].

Annex ZC (normative): UUI Header Field

For the purpose of the present document annex ZC is added.

ZC.1 Introduction

This annex defines the use of the UUI Header Field for use within SIP URI and Tel URI.

Editor's note: This annex is based on draft-johnston-sipping-cc-uui-02.txt and can be removed when the internet draft becomes an RFC and the usage of the UUI is allowed for SIP Methods and Responses. If this solution does not become an RFC, this parameter will be documented in the present document.

The UUI is represented header field parameter in a SIP request or response as described as follows.

The ABNF syntax is as follows:

```
The User-to-User header field can be present in INVITE requests and
responses only and in BYE requests and responses.


The following syntax specification uses the augmented Backus-Naur
Form (BNF) as described in RFC 2234 and extends RFC 3261.


      UUI             = "User-to-User" HCOLON uuidata *(SEMI uui-param)
      uuidata         = token
      uui-param       = enc-param | generic-param
      enc-param       = "encoding=" ("hex" | token)


The only defined parameter for the User-to-User header field is the
encoding parameter. "encoding=hex" is used to indicate that the UUI
information is encoded as hex digits.  Other encoding methods may
also be standardized.
```

ZC.2 Procedures at the terminating network

The UUI Header Field is a transparent field including information sent end to end. Based on operator policy the UUI header field may be deleted by the S-CCF or at the network boundary.

ZC.3 Extensions needed in table A.4 of ES 283 003

Table A.4: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
XX	an extension to the session initiation protocol foe UUI information?	[xx]	o (note)	cxx
cxx	A.3/2 OR A.3/3 OR A.3/4 OR A.3.5 OR A.3/6 OR A.3/7 OR A.3/8 OR A.3/9 OR A.3/10 OR A.3/11 THEN o ELSE n/a - - UUI Header Field			
NOTE:	It has to be clarified within the draft that the cpc value belongs to the trust domain and shall not be populated by UE's			

ZC.4 Extensions needed in table A.162 of ES 283 003

Table A.162: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
XX	an extension to the session initiation protocol for request UUI information?	[xx]	o (note)	cxx
cxx	A.3/2 OR A.3/3 OR A.3/4 OR A.3.5 OR A.3/6 OR A.3/7 OR A.3/8 OR A.3/9 OR A.3/10 OR A.3/11 THEN o ELSE n/a - - UUI Header Field			
NOTE:	It has to be clarified within the draft that the cpc value belongs to the trust domain and shall not be populated by UE's			

Annex ZD (normative): XML schema for PSTN

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://uri.etsi.org/ngn/params/xml/simservs/pstn"
xmlns:ns1="http://uri.etsi.org/ngn/params/xml/simservs/ pstn"
targetNamespace="http://uri.etsi.org/ngn/params/xml/simservs/ pstn"
elementFormDefault="qualified">
    <xs:annotation>
        <xs:documentation>XML Schema definition for mapping of some PSTN into SIP MIME
Bodies</xs:documentation>
    </xs:annotation>
    <!--Definition of simple types-->
    <xs:simpleType name="OneBitType">
        <xs:restriction base="xs:string">
            <xs:pattern value="[0-1]"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="TwoBitType">
        <xs:restriction base="xs:string">
            <xs:pattern value="[0-1][0-1]"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="ThreeBitType">
        <xs:restriction base="xs:string">
            <xs:pattern value="[0-1][0-1][0-1]"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="FourBitType">
        <xs:restriction base="xs:string">
            <xs:pattern value="[0-1][0-1][0-1][0-1]"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="FiveBitType">
        <xs:restriction base="xs:string">
            <xs:pattern value="[0-1][0-1][0-1][0-1][0-1]"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="SixBitType">
        <xs:restriction base="xs:string">
            <xs:pattern value="[0-1][0-1][0-1][0-1][0-1][0-1]"/>
        </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="SevenBitType">
        <xs:restriction base="xs:string">
            <xs:pattern value="[0-1][0-1][0-1][0-1][0-1][0-1][0-1]"/>
        </xs:restriction>
    </xs:simpleType>
```

```
<!--Definition of complex types-->
<!--Definition of BearerCapability Octets-->
<xs:complexType name="BCOctet3Type">
   <xs:sequence>
      <xs:element name="CodingStandard" type="TwoBitType"/>
      <xs:element name="InformationTransferCabability" type="FiveBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="BCOctet4Type">
   <xs:sequence>
      <xs:element name="TransferMode" type="TwoBitType"/>
      <xs:element name="InformationTransferRate" type="FiveBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="BCOctet4-1Type">
   <xs:sequence>
      <xs:element name="RateMultiplier" type="SevenBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="BCOctet5Type">
   <xs:sequence>
      <xs:element name="Layer1Identification" type="TwoBitType"/>
      <xs:element name="UserInfoLayer1Protocol" type="FiveBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="BCOctet5aType">
   <xs:sequence>
      <xs:element name="SynchronousAsynchronous" type="OneBitType"/>
      <xs:element name="Negotiation" type="OneBitType"/>
      <xs:element name="UserRate" type="FiveBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="BCOctet5bV110Type">
   <xs:sequence>
      <xs:element name="IntermediateRate" type="TwoBitType"/>
      <xs:element name="NIConTX" type="OneBitType"/>
      <xs:element name="NIConRX" type="OneBitType"/>
      <xs:element name="FlowControlOnTX" type="OneBitType"/>
      <xs:element name="FlowControlOnRX" type="OneBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="BCOctet5bV120Type">
   <xs:sequence>
      <xs:element name="RateAdaptionHeader" type="OneBitType"/>
      <xs:element name="MultipleFrameEstablishmentSupport" type="OneBitType"/>
      <xs:element name="ModeOfOperation" type="OneBitType"/>
      <xs:element name="LogicalLinkIdentifier" type="OneBitType"/>
      <xs:element name="Assignor" type="OneBitType"/>
      <xs:element name="InbandOutbandNegotiation" type="OneBitType"/>
   </xs:sequence>
</xs:complexType>
```

```
<xs:complexType name="BCOctet5cType">
   <xs:sequence>
      <xs:element name="NumberOfStopBits" type="TwoBitType"/>
      <xs:element name="NumberOfDataBits" type="TwoBitType"/>
      <xs:element name="Parity" type="ThreeBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="BCOctet5dType">
   <xs:sequence>
      <xs:element name="DuplexMode" type="OneBitType"/>
      <xs:element name="ModemType" type="SixBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="BCOctet6Type">
   <xs:sequence>
      <xs:element name="Layer2Identification" type="TwoBitType"/>
      <xs:element name="UserInfoLayer2Protocol" type="FiveBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="BCOctet7Type">
   <xs:sequence>
      <xs:element name="Layer3Identification" type="TwoBitType"/>
      <xs:element name="UserInfoLayer3Protocol" type="FiveBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="BCOctet7aType">
   <xs:sequence>
      <xs:element name="AdditionalLayer3Info" type="FourBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="BCOctet7bType">
   <xs:sequence>
      <xs:element name="AdditionalLayer3Info" type="FourBitType"/>
   </xs:sequence>
</xs:complexType>
<!--Definition of High Layer Compatibility Octets-->
<xs:complexType name="HLOctet3Type">
   <xs:sequence>
      <xs:element name="CodingStandard" type="TwoBitType"/>
      <xs:element name="Interpretation" type="ThreeBitType"/>
      <xs:element name="PresentationMethod" type="TwoBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="HLOctet4Type">
   <xs:sequence>
      <xs:element name="HighLayerCharacteristics" type="SevenBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="HLOctet4aMaintenanceType">
   <xs:sequence>
      <xs:element name="HighLayerCharacteristics" type="SevenBitType"/>
```

```
    </xs:sequence>
</xs:complexType>
<xs:complexType name="HLOctet4aAudioType">
    <xs:sequence>
        <xs:element name="VideoTelephonyCharacteristics" type="SevenBitType"/>
    </xs:sequence>
</xs:complexType>
<!--Definition of Low Layer Compatibility Octets-->
<xs:complexType name="LLOctet3Type">
    <xs:sequence>
        <xs:element name="CodingStandard" type="TwoBitType"/>
        <xs:element name="InformationTransferCapability" type="FiveBitType"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet3aType">
    <xs:sequence>
        <xs:element name="NegotiationIndicator" type="OneBitType"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet4Type">
    <xs:sequence>
        <xs:element name="TransferMode" type="TwoBitType"/>
        <xs:element name="InformationTransferRate" type="FiveBitType"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet4-1Type">
    <xs:sequence>
        <xs:element name="RateMultiplier" type="SevenBitType"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet5Type">
    <xs:sequence>
        <xs:element name="Layer1Identification" type="TwoBitType"/>
        <xs:element name="UserInfoLayer1Protocol" type="FiveBitType"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet5aType">
    <xs:sequence>
        <xs:element name="SynchronousAsynchronous" type="OneBitType"/>
        <xs:element name="Negotiation" type="OneBitType"/>
        <xs:element name="UserRate" type="FiveBitType"/>
    </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet5bV110Type">
    <xs:sequence>
        <xs:element name="IntermediateRate" type="TwoBitType"/>
        <xs:element name="NIConTX" type="OneBitType"/>
        <xs:element name="NIConRX" type="OneBitType"/>
        <xs:element name="FlowControlOnTX" type="OneBitType"/>
        <xs:element name="FlowControlOnRX" type="OneBitType"/>
    </xs:sequence>
```

```
</xs:complexType>
<xs:complexType name="LLOctet5bV120Type">
   <xs:sequence>
      <xs:element name="RateAdaptionHeader" type="OneBitType"/>
      <xs:element name="MultipleFrameEstablishmentSupport" type="OneBitType"/>
      <xs:element name="ModeOfOperation" type="OneBitType"/>
      <xs:element name="LogicalLinkIdentifier" type="OneBitType"/>
      <xs:element name="Assignor" type="OneBitType"/>
      <xs:element name="InbandOutbandNegotiation" type="OneBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet5cType">
   <xs:sequence>
      <xs:element name="NumberOfStopBits" type="TwoBitType"/>
      <xs:element name="NumberOfDataBits" type="TwoBitType"/>
      <xs:element name="Parity" type="ThreeBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet5dType">
   <xs:sequence>
      <xs:element name="DuplexMode" type="OneBitType"/>
      <xs:element name="ModemType" type="SixBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet6Type">
   <xs:sequence>
      <xs:element name="Layer2Identification" type="TwoBitType"/>
      <xs:element name="UserInfoLayer2Protocol" type="FiveBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet6aHDLCType">
   <xs:sequence>
      <xs:element name="Mode" type="TwoBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet6aUserSpecificType">
   <xs:sequence>
      <xs:element name="UserSpecificLayer2Information" type="SevenBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet6bType">
   <xs:sequence>
      <xs:element name="WindowSize" type="SevenBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet7Type">
   <xs:sequence>
      <xs:element name="Layer3Identification" type="TwoBitType"/>
      <xs:element name="UserInfoLayer3Protocol" type="FiveBitType"/>
   </xs:sequence>
</xs:complexType>
```

```
<xs:complexType name="LLOctet7aUserSpecificType">
   <xs:sequence>
      <xs:element name="OptionalLayer3Information" type="SevenBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet7aX25Type">
   <xs:sequence>
      <xs:element name="Mode" type="TwoBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet7bX25Type">
   <xs:sequence>
      <xs:element name="DefaultPacketSize" type="FourBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet7cType">
   <xs:sequence>
      <xs:element name="PacketWindowSize" type="SevenBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet7aTR9577Type">
   <xs:sequence>
      <xs:element name="AdditionalLayer3Info" type="FourBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="LLOctet7bTR9577Type">
   <xs:sequence>
      <xs:element name="AdditionalLayer3Info" type="FourBitType"/>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="DispOctet3Type">
   <xs:sequence>
      <xs:element name="DisplayInformation" type="SevenBitType"/>
   </xs:sequence>
</xs:complexType>
<!--Definition of the information elements-->
<xs:complexType name="BearerCapabilityType">
   <xs:sequence>
      <xs:element name="BCoctet3" type="BCOctet3Type"/>
      <xs:element name="BCoctet4" type="BCOctet4Type"/>
      <xs:element name="BCoctet4-1" type="BCOctet4-1Type" minOccurs="0"/>
      <xs:element name="BCoctet5" type="BCOctet5Type" minOccurs="0"/>
      <xs:element name="BCoctet5a" type="BCOctet5aType" minOccurs="0"/>
      <xs:element name="BCoctet5bV110" type="BCOctet5bV110Type" minOccurs="0"/>
      <xs:element name="BCoctet5bV120" type="BCOctet5bV120Type" minOccurs="0"/>
      <xs:element name="BCoctet5c" type="BCOctet5cType" minOccurs="0"/>
      <xs:element name="BCoctet5d" type="BCOctet5dType" minOccurs="0"/>
      <xs:element name="BCoctet6" type="BCOctet6Type" minOccurs="0"/>
      <xs:element name="BCoctet7" type="BCOctet7Type" minOccurs="0"/>
      <xs:element name="BCoctet7a" type="BCOctet7aType" minOccurs="0"/>
      <xs:element name="BCoctet7b" type="BCOctet7bType" minOccurs="0"/>
```

```
      </xs:sequence>
   </xs:complexType>
   <xs:complexType name="HighLayerCompatibilityType">
      <xs:sequence>
         <xs:element name="HLOctet3" type="HLOctet3Type"/>
         <xs:element name="HLOctet4" type="HLOctet4Type"/>
         <xs:element name="HLOctet4aMaintenance" type="HLOctet4aMaintenanceType"
minOccurs="0"/>
         <xs:element name="HLOctet4Audio" type="HLOctet4aAudioType" minOccurs="0"/>
      </xs:sequence>
   </xs:complexType>
   <xs:complexType name="LowLayerCompatibilityType">
      <xs:sequence>
         <xs:element name="LLOctet3" type="LLOctet3Type"/>
         <xs:element name="LLOctet3a" type="LLOctet3aType" minOccurs="0"/>
         <xs:element name="LLOctet4" type="LLOctet4Type"/>
         <xs:element name="LLOctet4-1" type="LLOctet4-1Type" minOccurs="0"/>
         <xs:element name="LLOctet5" type="LLOctet5Type" minOccurs="0"/>
         <xs:element name="LLOctet5a" type="LLOctet5aType" minOccurs="0"/>
         <xs:element name="LLOctet5bV110" type="LLOctet5bV110Type" minOccurs="0"/>
         <xs:element name="LLOctet5bV120" type="LLOctet5bV120Type" minOccurs="0"/>
         <xs:element name="LLOctet5c" type="LLOctet5cType" minOccurs="0"/>
         <xs:element name="LLOctet5d" type="LLOctet5dType" minOccurs="0"/>
         <xs:element name="LLOctet6" type="LLOctet6Type" minOccurs="0"/>
         <xs:element name="LLOctet6aHDLC" type="LLOctet6aHDLCType" minOccurs="0"/>
         <xs:element name="LLOctet6aUserSpecific" type="LLOctet6aUserSpecificType"
minOccurs="0"/>
         <xs:element name="LLOctet6b" type="LLOctet6bType" minOccurs="0"/>
         <xs:element name="LLOctet7" type="LLOctet7Type"/>
         <xs:element name="LLOctet7aUserSpecific" type="LLOctet7aUserSpecificType"
minOccurs="0"/>
         <xs:element name="LLOctet7aX25" type="LLOctet7aX25Type" minOccurs="0"/>
         <xs:element name="LLOctet7bX25" type="LLOctet7bX25Type" minOccurs="0"/>
         <xs:element name="LLOctet7c" type="LLOctet7cType" minOccurs="0"/>
         <xs:element name="LLOctet7aTR9577" type="LLOctet7aTR9577Type"
minOccurs="0"/>
         <xs:element name="LLOctet7bTR9577" type="LLOctet7bTR9577Type"
minOccurs="0"/>
      </xs:sequence>
   </xs:complexType>
   <xs:complexType name="DisplayType">
      <xs:sequence>
         <xs:element name="DispOctet3" type="DispOctet3Type"/>
      </xs:sequence>
   </xs:complexType>
   <!--Definition of progress indicator-->
   <xs:complexType name="ProgressOctet3Type">
      <xs:sequence>
         <xs:element name="CodingStandard" type="TwoBitType"/>
         <xs:element name="Location" type=" FourBitType "/>
      </xs:sequence>
```

```
    </xs:complexType>
    <xs:complexType name="ProgressOctet4Type">
        <xs:sequence>
            <xs:element name="ProgressDescription" type="SevenBitType"/>
        </xs:sequence>
    </xs:complexType>
    <xs:complexType name="ProgressIndicatorType">
        <xs:sequence>
            <xs:element name="ProgressOctet3" type="ProgressOctet3Type"/>
            <xs:element name="ProgressOctet4" type="ProgressOctet4Type"/>
        </xs:sequence>
    </xs:complexType>
    <!--Definition of document structure-->
    <xs:element name="PSTN-transit">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="BearerInfomationElement" type="BearerCapabilityType"
maxOccurs="2"/>
                <xs:element name="HighLayerCompatibility" type="HighLayerCompatibilityType"
minOccurs="0" maxOccurs="2"/>
                <xs:element name="LowLayerCompatibility" type="LowLayerCompatibilityType"
minOccurs="0"/>
                <xs:element name="ProgressIndicator" type="ProgressIndicatorType" minOccurs="0"
maxOccurs="unbounded"/>
                <xs:element name="Display" type="DisplayType" minOccurs="0"
maxOccurs="unbounded"/>
            </xs:sequence>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

Annex ZE (informative): Change history

TISPAN #	TISPAN Doc.	CR	Subject/Comment
	13tTD440r3	001	WI03120, CR001: mandate the authorization header in case of HTTP Digest Authentication mechanism This CR was agreed during TISPAN#13Ter and revised in TISPAN#14Bis (14bTD077).
	14bTD239r4	002	WI03120, CR002: Addition of the Reason Header within Responses. This CR was agreed during TISPAN#14Bis.
	14tTD288r3	003	WI03120, CR003: Upgrading ES 283 003 to take 3GPP TS 24.229 [1] v7.8.0 as basis.
	14Ttd288r4	003	Minor update to CR3 as discussed on TISPAN_GEN list during CR approval process: subclause 5.1.1.2, item j) was underlined. This text is already included in 24.229 version 7.8.0, and therefore should be shown as plain text.
	15bTD066r2	004	WI03120, CR004: included some editorial changes.
	15bTD304r1	006	WI3120, CR006: addition of UUI Header for User to User Service.
TISPAN3-WG3	WG3TD121r3	007	WI3120 ES 283 003 SIP XML addition for support of transit specific content
TISPAN3-WG3	WG3TD119r1	008	Alignment with Release1 on the usage of port for SIP messages without security association
TISPAN3-WG3	WG3TD122r1	009	Correction of incorrect implementation of CR in clause 5.4.1.2A
TISPAN3-WG3	void	010	void
TISPAN3-WG3	WG3TD125r1	011	Clarification in clause 5.1.1.7 Network initiated deregistration
TISPAN3-WG3	WG3TD130r1	012	Alignment of text in clause 5.4.1.2A
TISPAN3-WG3	WG3TD148r2	013	Keep Alive for Signalling
TISPAN3-WG3	WG3TD149r1	014	ES 283 003 Add NAT traversal for media to the endorsement of 24.229
TISPAN3-WG3	WG3TD179r2	015	WI3120 ES 283 003 Harmonization of Digest authentication
TISPAN3-WG3	WG3TD197r1	016	Endorsement of annexes and correction of references
TISPAN3-WG3	WG3TD226	017	Scope limitation

History

Document history		
V1.1.1	July 2006	Publication
V1.8.0	September 2007	Publication
V2.5.1	January 2008	Membership Approval Procedure MV 20080321: 2008-01-22 to 2008-03-21
V2.5.1	April 2008	Publication