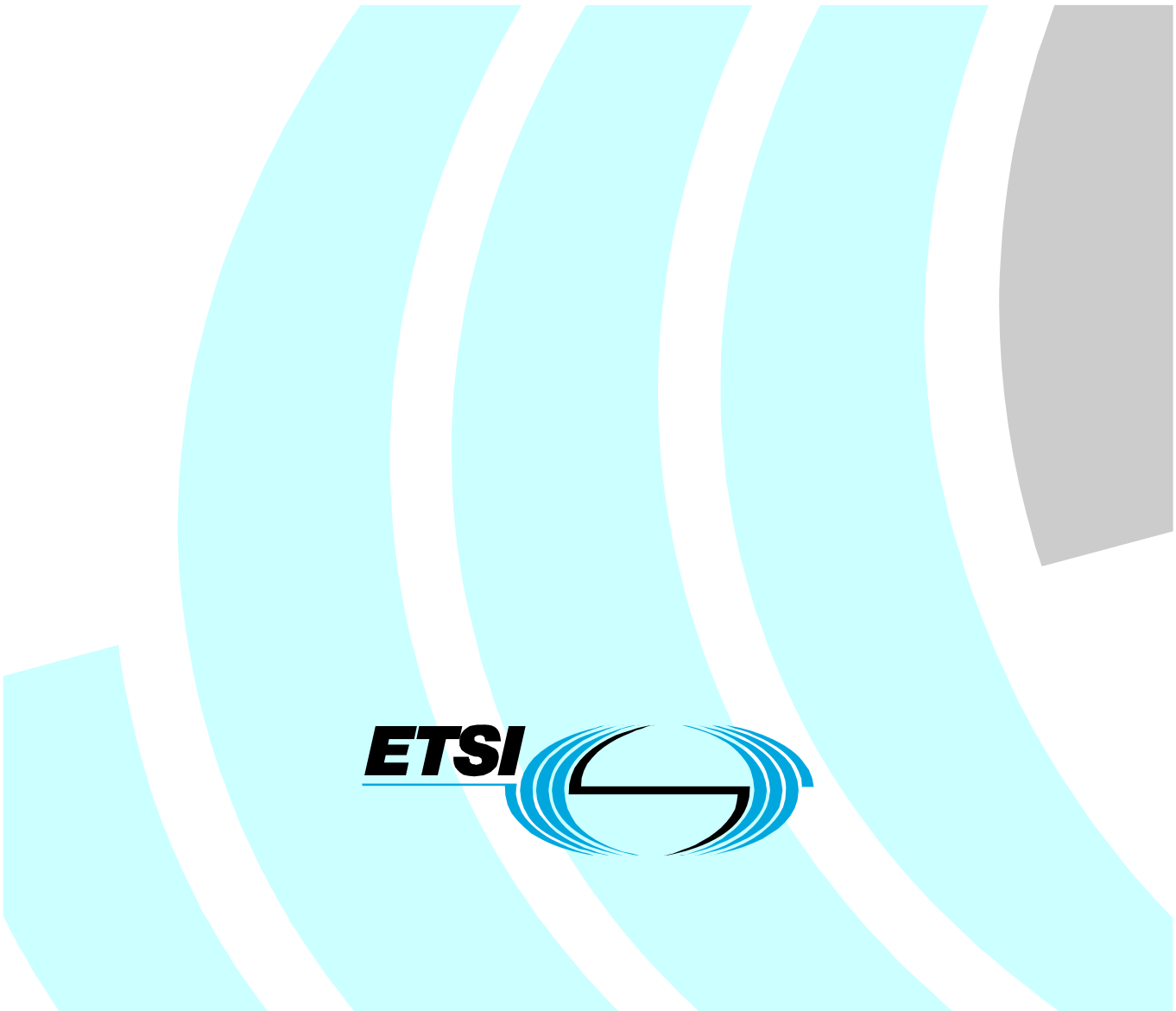
Final draft ETSI ES 283 003 V1.8.0 (2007-07)

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-03092-NGN-R1

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), and is now submitted for the ETSI standards Membership Approval Procedure.

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.

2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

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

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

[1] 3GPP TS 24.229 (V7.2.0): "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 (Release 7)".

[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 (V7.2.0): "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 (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 3 of [1] is replaced by the clause 3 shown in the present document.

For the purpose of the present document clause 4 of [1] applies, except for subclauses 4.1, 4.2, 4.3 and 4.4, which are replaced by the appropriate subclauses in clause 4 of the present document.

For the purpose of the present document clause 5 of [1] applies, except for subclauses 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, 5.1.1.5.A, 5.1.1.6, 5.1.1.7, 5.1.2A.1, 5.1.2.A.2, 5.1.6, 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, 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, 5.6.2, 5.10.1, 5.10.2.2, 5.10.2.3 and 5.10.3.1, which are replaced by the appropriate subclauses in clause 5 of the present document. In addition subclauses 5.1.1.1B, 5.1.1.2A, 5.1.1.4A, 5.1.1.5.1A, 5.1.1.6A, 5.2.2A, 5.4.1.2A.1, 5.4.8, 5.10.6 and 5.11 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 subclauses in clause 6 of the present document.

For the purpose of the present document clause 7 of [1] applies, except for subclauses 7.2A.4, 7.6.2 and 7.6.3 which are replaced by the appropriate subclauses in clause 7 of the present document.

For the purpose of the present document clause 9 of [1] applies, except for subclause 9.2.2, which are replaced by the appropriate subclauses in clause 9 of the present document.

For the purpose of the present document annex A of [1] applies, except for subclauses A.1.3, A.2.1.2, A.2.1.4.1, A.2.2.2 and A.2.2.4.1, and A.3.2.1 which are replaced by the appropriate subclauses in annex A of the present document.

For the purpose of the present document annex B of [1] applies, except for the addition of clauses B.2.2.6 and B.3.1.1 described in the appropriate subclauses in annex B of the present document.

For the purpose of the present document annex C of [1] applies, except for the addition of clause C.4 described in the appropriate subclauses in annex C of the present document.

For the purpose of the present document annex D of [1] applies, except for the addition of clauses D.2.2.6 and D.3.1.1 described in the appropriate subclauses in annex D of the present document.

For the purpose of the present document annex E of [1] applies, except for the addition of clauses E.2.2.6 and E.3 described in the appropriate subclauses in annex E of the present document.

Global modifications to 3GPP TS 24.229

The scope in clause 1 of [1] should be extended with applicability to:

- the interface between the CSCF and an IBCF.

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

Replace references as shown below.

Reference in TS 24.229 [1]	Modified reference
[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 1" (note 1)
[4A] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture"	(note 2)
[4B] 3GPP TS 23.167: "IP Multimedia Subsystem (IMS) emergency session; Stage 2"	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)
[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 (3GPP TS 23.228 v7.2.0, modified)" (note 1)
[8] 3GPP TS 24.141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3"	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)

Reference in TS 24.229 [1]	Modified reference
[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 v6.3.0, 3GPP TS 32.260 v6.3.0, 3GPP TS 32.297 v6.1.0, 3GPP TS 32.298 v6.1.0 and 3GPP TS 32.299 v6.4.0 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 v6.3.0, 3GPP TS 32.260 v6.3.0, 3GPP TS 32.297 v6.1.0, 3GPP TS 32.298 v6.1.0 and 3GPP TS 32.299 v6.4.0 modified]" (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: Draft-ietf-sip-acr-code-04 NOTE: The document cannot be formally referenced until it is published as an RFC. (note 1)
[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)
[91] draft-ietf-ecrit-requirements-09 (May 2006): "Requirements for Emergency Context Resolution with Internet Technologies" (note 3)	New reference: draft-ietf-ecrit-requirements-13 NOTE: The document cannot be formally referenced until it is published as an RFC. (note 1)
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 specific requirements and is not generally applicable to the present endorsement. NOTE 3: This reference is available in 3GPP TS 24.229 (V7.5.0).	

3 Definitions and abbreviations

3.1 Definitions

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

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

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

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

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

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

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

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

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

Emergency registration: A special registration that relates to an emergency public user identity.

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

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

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

Fully-Qualified Domain Name (FQDN)

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

Back-to-Back User Agent (B2BUA)
Client
Dialog
Final response
Header
Header field
Loose routeing
Method
Option-tag (see RFC 3261 [26] subclause 19.2)
Provisional response
Proxy, proxy server
Recursion
Redirect server
Registrar
Request
Response
Server
Session
(SIP) transaction
Stateful proxy
Stateless proxy
Status-code (see RFC 3261 [26] subclause 7.2)
Tag (see RFC 3261 [26] subclause 19.3)
Target Refresh Request

User agent client (UAC)
User agent server (UAS)
User agent (UA)

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

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

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

Filter criteria
Initial filter criteria
Initial request
Standalone transaction
Subsequent request

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

Border control concepts
Interconnection Border Control Function (IBCF)
Interrogating-CSCF (I-CSCF)
IMS Application Level Gateway (IMS-ALG)
IP-Connectivity Access Network (IP-CAN)
Policy Decision Function (PDF)
Private user identity
Proxy-CSCF (P-CSCF)
Public Service Identity (PSI)
Public user identity
Serving-CSCF (S-CSCF)
Statically pre-configured PSI

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

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

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

IM Subscriber Identity Module (ISIM)
Protected server port
Protected client port

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

Universal Integrated Circuit Card (UICC)
Universal Subscriber Identity Module (USIM)
User Equipment (UE)

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

Security association

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

i) the security association that exists between the UE and the P-CSCF. This is the only security association that has direct impact on SIP; or

ii) the security association that exists between the WLAN UE and the PDG. This is the security association that is relevant to the discussion of Interworking WLAN as the underlying IP-CAN.

For the purposes of the present document, the following terms and definitions given in 3GPP TS 23.002 [1B] apply:

WLAN UE
3GPP AAA proxy
3GPP AAA server
Packet Data Gateway (PDG)

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

Interworking WLAN

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

International public telecommunication number

For the purposes of the present document, the following terms and definitions given in draft-ietf-ecrit-requirements [91] apply:

Emergency service identifier
Emergency service URN
Public Safety Answering Point (PSAP)
PSAP URI

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
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTD	Document Type Definition
EC	Emergency Centre
ECF	Event Charging Function
E-CSCF	Emergency CSCF
ESRP	Emergency Service Routeing Proxy
FQDN	Fully Qualified Domain Name
GCID	GPRS Charging Identifier
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service

~~HSS~~	~~Home Subscriber Server~~
i	irrelevant
IBCF	Interconnection Border Control Function
I-CSCF	Interrogating CSCF
ICID	IM CN subsystem Charging 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
P-CSCF	Proxy CSCF
PDF	Policy Decision Function
PDG	Packet Data Gateway
PDP	Packet Data Protocol
PDU	Protocol Data Unit
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-CSCF	Serving CSCF
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

UDVM	Universal Decompressor Virtual Machine
UPSF	User Profile Server Function
USIM	Universal Subscriber Identity Module
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 subsytem functional entity using an interface at the Gm 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 Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Mm reference point and the Mw reference point are defined in 3GPP TS 23.002 [2].

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

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

- The User Equipment (UE) shall provide the User Agent (UA) role, with the exceptions and additional capabilities to SIP as described in subclause 5.1, with the exceptions and additional capabilities to SDP as described in subclause 6.1, and with the exceptions and additional capabilities to SigComp as described in subclause 8.1. The UE shall also provide the access dependent procedures 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 the P-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.

- The I-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.3.

- The S-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.4, and with the exceptions and additional capabilities to SDP as described in subclause 6.3. Under certain circumstances as described in subclause 5.4, the S-CSCF shall provide the UA role with the additional capabilities, as follows:

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

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

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

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

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

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

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.

4.2 URI and address assignments

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

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

2) All IM CN subsystem entities are allocated IP addresses. For systems providing access to IMS using a fixed broadband interconnection, 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: 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) 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.

6) 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~~7) For the purpose of emergency service, the UE shall use at least two emergency public user identities, of which one is a SIP URI derived as specified in 3GPP TS 23.003 [3] and the second is a tel URI.

4.2A Transport mechanisms

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

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

4.3 Routeing principles of IM CN subsystem entities

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

4.4 Trust domain

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

Editor's Note: The exact mechanism to determine which nodes are part of the trust domain and which nodes are not, is FFS.

NOTE 1: For the purpose of this document, the PSAP is automatically regarded as being within the trust domain. This means that e.g. the handling of the P-Access-Network-Info header, P-Asserted-Identity header and the History-Info header will be as if the PSAP is within the trust domain, and these header fields will not be removed for trust domain issues.

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

NOTE 2: In addition to the procedures specified in clause 5, procedures of RFC 3325 [34] in relation to transmission of P-Asserted-Identity headers and their contents outside the trust domain also apply.

According to draft-ietf-sip-history-info [66] subclause 3.3, the History-Info header can be restricted to specific domains. Therefore for the purpose of the History-Info header within this specification, a trust domain also applies. This trust domain is identical to that of the P-Asserted-Identity. For the History-Info header, subclause 5.4 also identifies additional cases for the removal of the header. SIP functional entities within the trust domain will need to take an action on the removal of the History-Info header when SIP signalling crosses the boundary of the trust domain.

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. After a successful registration, the UE will get the associated public user identities, and the UE may use any of them in subsequent non-REGISTER requests.

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

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 UE can register a public user identity with its contact address at any time after it has aquired 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;

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 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. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the sent-by field;

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

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

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

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) the Security-Client header field set to specify the security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];

i) the Supported header containing the option tag "path"; and

j) if a security association exists, 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; and

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.

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

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

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.

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

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) the Supported header containing the option tag "path"; 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;

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

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

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

5.1.1.3 Initial subscription to the registration-state event package

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

The UE shall use the default public user identity for subscription to the registration-state event package, if the public user identity that was used for initial registration is a barred public user identity. The UE may use either the default public user identity or the public user identity used for initial registration for the subscription to the registration-state event package, if the initial public user identity that was used for 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.

5.1.1.4 User-initiated re-registration (with security association)

The UE can reregister a previously registered public user identity with its contact address at any time.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less, or when the UE intends to update its capabilities according to RFC 3840 [62].

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

The UE shall extract or derive 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 field set to the value of the 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 protected server port value bound to the security association;

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.

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

f) an Expires header, or an expires parameter within the Contact header, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

i) a Security-Verify header that contains the content of the Security-Server header received in the 401 (Unauthorized) response of the last successful authentication;

j) the Supported header containing the option tag "path"; and

k) <u>if available to the UE (as defined in the access technology specific annexes for each access technology),</u> 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; and

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.

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

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

<u>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.</u>

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.

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.

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.

5.1.1.4A User-initiated re-registration without security association

The UE can reregister a previously registered public user identity with its contact address at any time.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less, or when the UE intends to update its capabilities according to RFC 3840 [62].

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;

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

g) a Request-URI set to the SIP URI of the domain name of the home network;

h) the Supported header containing the option tag "path"; 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;

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

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.

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 achieved via the registration and re-registration procedures as defined in subclause 5.1.1.2 and 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 as the shared key. The UE shall use the parameters received in the Security-Server header to setup the temporary set of security associations. The UE shall set a temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and

3) send another REGISTER request using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the 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 integrity protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the integrity protected REGISTER request, the UE shall:

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

- use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

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

5.1.1.5A 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 integrity protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if one is available.

The UE shall extract or derive 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 field, set to the value of the 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 the protected server port value bound to the security association;

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; 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 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 field, 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;

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 set to "rejected" or "deactivated"; or

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

the UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the initial registration procedure as described in subclause 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) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header contains the value of "terminated"; 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 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, then the UE considers the subscription to the reg event package terminated (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero, or a NOTIFY request was received with Subscription-State header containing the value of "terminated").

NOTE 3: When the P-CSCF has removed the security association established between the P-CSCF and the UE, further SIP signalling (e.g. the NOTIFY containing the deregistration event) will not reach the UE.

5.1.2A.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:

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

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 integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

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

NOTE 1: Since the S-CSCF 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 implict registration that was not subsequently deregistered or has expired; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

NOTE 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".

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 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 ~~. The UE shall populate the P-Access-Network-Info header with the current point of attachment to the IP-CAN as specified for the access network technology~~ (see subclause 7.2A.4).

NOTE 6: 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.

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

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, when the UE sends any response, the UE shall:

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

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.

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 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. ~~The UE shall populate the P-Access-Network-Info header with its current point of attachment to the IP-CAN as specified for the access network technology~~ (see subclause 7.2A.4).

5.1.6 Emergency service

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

~~In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a XML body that includes an <alternative service> element with the <type> child element set to "emergency", the UE shall automatically:~~

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

~~The UE may also provide an indication to the user based on the text string contained in the <reason> element.~~

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

5.1.6.1 General

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup according to the procedures described in 3GPP TS 24.008 [8].

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered, the UE shall attempt an emergency call as described in subclause 5.1.6.8.4.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is not currently registered, the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is attached to a different network than its home operator's network (e.g. VPLMN) and the assigned P-CSCF is located in its home operator's network (e.g. in the HPLMN), the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE has no credentials the UE can make an emergency call without being registered. The UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

The IP-CAN can, dependant on the IP-CAN capabilities, provide local emergency numbers to the UE which has that capability, in order for the UE to recognize these numbers as emergency call.

5.1.6.2 Initial emergency registration

When the user initiates an emergency call, if emergency registration is needed, the UE shall perform an emergency registration prior to sending the SIP request related to the emergency call.

When a UE performs an initial emergency registration the UE shall perform the actions as specified in subclause 5.1.1.2 with the following additions:

- the UE shall populate the To and From header in the REGISTER request with the emergency public user identity as specified in 3GPP TS 23.003 [3].

When the UE performs an initial emergency registration and whilst this emergency registration is active, the UE shall:

- handle the emergency registration independently from any other ongoing registration to the IM CN subsystem;
- handle any signalling or media related IP-CAN for the purpose of emergency calls independently from any other established IP-CAN for IM CN subsystem related signalling or media; and
- handle all SIP signalling and all media related to the emergency call independently from any other ongoing IM CN subsystem signalling and media.

5.1.6.2A New initial emergency registration

The UE shall perform a new initial emergency registration, as specified in subclause 5.1.6.2, if the UE determines that:

- it has previously performed an emergency registration which has not yet expired; and
- it has obtained an IP address from the serving IP-CAN, as specified in subclause 9.2.1, different than the IP address used for the emergency registration.

5.1.6.3 Initial subscription to the registration-state event package

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

5.1.6.4 User-initiated emergency reregistration

The UE shall perform user-initiated emergency reregistration as specified in subclause 5.1.1.4 if:

- half of the time for the emergency registration has expired and the UE has emergency related ongoing dialog or if standalone transactions exist; or
- the user initiates an emergency call.

The UE shall not perform user-initiated emergency reregistration in any other cases.

5.1.6.5 Authentication

When a UE performs authentication a UE shall perform the procedures as specified in subclause 5.1.1.5.

5.1.6.6 User-initiated emergency deregistration

The UE shall not perform user-initiated deregistration of any registered emergency public user identity.

NOTE: The UE will be deregistered when the emergency registration expires.

5.1.6.7 Network-initiated emergency deregistration

An emergency registration will not be deregistered by the network (see subclause 5.4.8.4).

5.1.6.8 Emergency session setup

5.1.6.8.1 General

The UE shall translate any user indicated emergency number as specified in 3GPP TS 22.101 [1A] to an emergency service URN, i.e. an URN with "sos" service type as specified in draft-ietf-ecrit-service-urn [69].

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a XML body that includes an <alternative service> element with the <type> child element set to "emergency", the UE shall automatically send an ACK request to the P-CSCF as per normal SIP procedures and terminate the session.

NOTE 1: The UE can attempt an emergency call setup according to the procedures described in 3GPP TS 24.008 [8].

NOTE 2: Emergency numbers which the UE does not detect, will be treated as a normal call.

5.1.6.8.2 Emergency session set-up in case of no registration

When establishing an emergency session for an unregistered user, the UE shall be allowed to receive responses to emergency requests and requests inside an established emergency session on the unprotected ports. All other messages not arriving on a protected port shall be rejected or silently discarded by the UE.

Prior to establishing an emergency session for an unregistered user, the UE shall acquire a local IP address, discover a P-CSCF, and establish an IP-CAN bearer that can be used for SIP signalling. The UE shall send only the initial INVITE requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial INVITE request to the SIP default port values as specified in RFC 3261 [26].

The UE shall apply the procedures as specified in subclause 5.1.2A.1 and subclause 5.1.3 with the following additions:

1) the UE shall set the From header field of the INVITE request to "Anonymous" as specified in RFC 3261 [26];

2) the UE shall include a Request-URI in the initial INVITE request that contains an emergency service URN, i.e. with "sos" service type as specified in draft ietf-ecrit-service-urn [69]. An additional sub-service type can be added if information on the type of emergency service is known;

NOTE 1: Other specifications make provision for emergency service identifiers, that are not specifically the emergency service URN, to be recognised in the UE. Emergency service identifiers which the UE does not detect will be treated as a normal call by the UE.

3) the UE shall insert in the INVITE request, a To header with:

- the same emergency service URN as in the Request URI; or

- if the UE cannot perform local dialstring interpretation for the dialled digits, a dialstring URI representing the dialled digits in accordance with draft-rosen-iptel-dialstring [103] or a tel URL representing the dialled digits;

NOTE 2: This version of the present document does not provide any specified handling of a URI with the dialled digits in accordance with draft-rosen-iptel-dialstring [103] at an entity within the IM CN susbsystem. Behaviour when this is used is therefore not defined.

4) if available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall include in the P-Access-Network-Info header in any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request. The UE shall populate the P-Access-Network-Info header with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4). The P-Access-Network-Info header contains the location identifier such as the cell id, the line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

5) the UE shall populate the P-Preferred-Identity header in the INVITE request with an equipment identifier as a SIP URI. The special details of the equipment identifier to use depends on the IP-CAN;

6) a Contact header set to include SIP URI that contains in the hostport parameter the IP address of the UE and an unprotected port where the UE will receive incoming requests belonging to this dialog;

7) a Via header set to include the IP address of the UE in the sent-by field and for the UDP the unprotected server port value where the UE will receive response to the emergency request, while for the TCP, the response is received on the TCP connection on which the emergency request was sent;

8) if the UE has its location information available, it shall include the location information in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header in accordance with draft-ietf-sip-location-conveyance [89]; or

- if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 [90] and include the location object in a message body with the content type application/pidf+xml in accordance with draft-ietf-sip-location-conveyance [89]. The Geolocation header is set to a Content ID in accordance with draft-ietf-sip-location-conveyance [89]; and

9) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in draft-ietf-sip-location-conveyance [89] in the INVITE request.

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

NOTE 4: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header 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. The UE shall build a Route header value containing only the P-CSCF URI (containing the unprotected port number and the IP address or the FQDN learnt through the P-CSCF discovery procedures).

In the event the UE receives a 380 (Alternative Service) response to an INVITE request containing a XML body that includes an <alternative service> element with the <type> child element set to "emergency" and an <action> child element, set to "emergency-registration", and the UE does not have sufficient credentials to authenticate with the IM CN subsystem, the UE shall not initiate an emergency registration.

NOTE 5: The UE can attempt an emergency call setup according to the procedures described in 3GPP TS 24.008 [8].

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

NOTE 6: It is an implementation option whether these actions are also triggered by other means.

NOTE 7: A number of 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.

NOTE 8: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

5.1.6.8.3 Emergency session set-up within an emergency registration

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclauses 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

1) the UE shall include a Request URI in the INVITE request that contains an emergency service URN, i.e. with "sos" service type as specified in draft-ietf-ecrit-service-urn [69]. An additional sub-service type can be added if information on the type of emergency service is known;

2) the UE shall insert in the INVITE request, a To header with:

   - the same emergency service URN as in the Request URI; or

   - if the UE cannot perform local dialstring interpretation for the dialled digits, a dialstring URI representing the dialled digits in accordance with draft-rosen-iptel-dialstring [103] or a tel URL representing the dialled digits;

NOTE 1: This version of the present document does not provide any specified handling of a URI with the dialled digits in accordance with draft-rosen-iptel-dialstring [103] at an entity within the IM CN susbsystem. Behaviour when this is used is therefore not defined.

3) the UE shall insert in the INVITE request, a From header that includes the public user identity or the tel URI associated with the public user identity, as described in subclause 4.2;

4) the UE shall insert in the INVITE request, a P-Preferred-Identity header that includes the emergency public user identity or the tel URI associated with the emergency public user identity as described in subclause 4.2;

5) if the UE has its location information available, it shall include it in the INVITE request in the following way:

   - if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header in accordance with draft-ietf-sip-location-conveyance [89]; or

   - if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 [90] and include the location object in a message body with the content type application/pidf+xml in accordance with draft-ietf-sip-location-conveyance [89]. The Geolocation header is set to a Content ID in accordance with draft-ietf-sip-location-conveyance [89];

NOTE 2: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

6) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in draft-ietf-sip-location-conveyance [89] in the INVITE request; and

7) if available to the UE, the P-Access-Network-Info header shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call.

NOTE 3: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

NOTE 4: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

5.1.6.8.4 Emergency session setup within a non-emergency registration

The UE shall apply the procedures as specified in subclauses 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

1) the UE shall include a Request URI in the INVITE request that contains an emergency service URN, i.e. with "sos" service type as specified in draft-ietf-ecrit-service-urn [69]. An additional sub-service type can be added if information on the type of emergency service is known;

2) the UE shall insert in the INVITE request, a To header with:

   - the same emergency service URN as in the Request URI; or

   - if the UE cannot perform local dialstring interpretation for the dialled digits, a dialstring URI representing the dialled digits in accordance with draft-rosen-iptel-dialstring [103] or a tel URL representing the dialled digits;

NOTE 1: This version of the present document does not provide any specified handling of a URI with the dialled digits in accordance with draft-rosen-iptel-dialstring [103] at an entity within the IM CN susbsystem. Behaviour when this is used is therefore not defined.

3) the UE shall insert in the INVITE request, a From header that includes the public user identity or the tel URI associated with the public user identity, as described in subclause 4.2;

4) the UE shall insert in the INVITE request a P-Preferred-Identity that includes the public user identity or the tel URI associated with the public user identity as described in subclause 4.2;

5) if the UE has its location information available, it shall include it in the INVITE request in the following way:

   - if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header in accordance with draft-ietf-sip-location-conveyance [89]; or

   - if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 [90] and include the location object in a message body with the content type application/pidf+xml in accordance with draft-ietf-sip-location-conveyance [89]. The Geolocation header is set to a Content ID in accordance with draft-ietf-sip-location-conveyance [89];

6) if available to the UE, the P-Access-Network-Info header shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call; and

7) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in draft-ietf-sip-location-conveyance [89] in the INVITE request.

NOTE 2: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

Upon receiving a 380 (Alternative Service) response to the INVITE request, with the 380 (Alternative Service) response include a IM CN subsystem XML body, with the type element set to "emergency" and the action element set to "emergency-registration" the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

Editor's Note: It is FFS how the UE will indicate if no location is available if the UE does not support draft-ietf-sip-location-conveyance [89].

NOTE 3: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

NOTE 4: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

5.1.6.9 Emergency session release

Normal call release procedure shall apply, as specified in the subclause 5.1.5.

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

NOTE 4: 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. When a security association was set up at registration, the P-CSCF will discard any SIP message that is not integrity protected and is received outside of the registration and authentication procedures. The integrity protection and checking requirements on the P-CSCF within the registration and authentication procedures are defined in subclause 5.2.2.

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. 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.

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 the initial REGISTER requests on the port advertised to the UE during the P-CSCF discovery procedure.

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

1) insert a Path header in the request including an entry containing:

   - the SIP URI identifying the P-CSCF;

   - an indication that requests routed in this direction of the path (i.e. from the S-CSCF 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];

4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value "yes" into the Authorization header field in case the REGISTER request was either received integrity protected with the security association created during an ongoing authentication procedure and includes an authentication challenge response (i.e. RES parameter), or it was received on the security association created during the last successful authentication procedure 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 integrity 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 integrity protected, then the P-CSCF shall:

   a) check the security association which protected the request. If the security association is a temporary one, then the request is expected to contain a Security-Verify header in addition to a Security-Client header. If there are no such headers, then the P-CSCF shall return a suitable 4xx response. If there are such headers, then the P-CSCF shall compare the content of the Security-Verify header with the content of the Security-Server header sent earlier and the content of the Security-Client header with the content of the Security-Client header received in the challenged REGISTER. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx response. If the contents match, the P-CSCF shall remove the Security-Verify and the Security-Client header;

   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-CSCF; and

c) check if the private user identity conveyed in the Authorization header of the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;

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

8) if the P-CSCF is located in the visited network, and local policy requires the ~~application of~~ IBCF capabilities~~concepts~~ in the visited network towards the home network, then ~~the P-CSCF shall~~ 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.

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 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 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

1) delete any temporary set of security associations established towards the UE;

2) remove the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and to the temporary set of security associations which will be setup as a result of this challenge. The P-CSCF shall forward the 401 (Unauthorized) response to the UE if and only if the CK and IK have been removed;

3) insert a Security-Server header in the response, containing the P-CSCF static security list and the parameters needed for the security association setup, as specified in Annex H of 3GPP TS 33.203 [19]. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms;

4) set up the temporary set of security associations with a temporary SIP level lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set the temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer; and

5) send the 401 (Unauthorized) response to the UE using the security association with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 4: The challenge in the 401 (Unauthorized) response sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up two pairs of security associations with the UE during the same registration procedure. For further details see 3GPP TS 33.203 [19].

When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall check the value of the Expires header field and/or Expires parameter in the Contact header. When the value of the Expires header field and/or expires parameter in the Contact header is different than zero, then the P-CSCF shall:

1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routeing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;

2) associate the Service-Route header list with the registered public user identity;

3) store the public user identities found in the P-Associated-URI header value and associate them to the 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 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 an existing set of security association is available, set the SIP level lifetime of the security association to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds;

7) if a 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

8) protect the 200 (OK) response to the REGISTER request within the same security association to that in which the request was protected.

When receiving a SIP message (including REGISTER requests) from the UE over the newly established set of security associations that have not yet been taken into use, the P-CSCF shall:

1) reduce the SIP level lifetime 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 6: 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 7: 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 8: 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-CSCF towards the P-CSCF) are expected to be treated as for the UE-terminating case. This indication may e.g. be in a parameter in the URI, a character string in the user part of the URI, or be a port number in the URI;

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];

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 IBCF capabilities ~~concepts~~ 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.

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 associated event attribute element 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 UEis 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-CSCF 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 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 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.

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 that may include a Warning header containing the warn-code 399; 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 4: 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 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, rewrite the port number of its own Record Route entry to its own protected server port number negotiated with the calling UE; and

NOTE ~~2~~5: 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 response may include a Warning header containing the warn-code 399. 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 that may include a Warning header containing the warn-code 399; 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 top of 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 ~~3~~6: 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 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 that may include a Warning header containing the warn-code 399; 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 7: How the IBCF exit point address is obtained by the P-CSCF is implementation dependent.

3) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request; and

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 response may include a Warning header containing the warn-code 399. 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 that may include a Warning header containing the warn-code 399; 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 that may include a Warning header containing the warn-code 399; 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) <u>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</u>

<u>NOTE 8: How the IBCF exit point address is obtained by the P-CSCF is implementation dependent.</u>

3) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

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

5.2.6.4 Requests terminated by the UE

When the P-CSCF receives, destined for the UE, an initial request for a dialog, prior to forwarding the request, the P-CSCF shall:

1) 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 value saved from the P-Called-Party-ID header that was received in the request;

2) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Via header values with those received in the request;

3) verify that the list of URIs received in the Record-Route header of the request corresponding to the same dialog is included, preserving the same order, as a subset of the Record-Route header list of this response. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) discard the response; or

   b) replace the Record-Route header values with those received in the request, if a security association exists rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter if present.

      If the verification is successful, the P-CSCF shall, if a security association exists, rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter if 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 <u>if a security association exists,</u> 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 <u>if a security association exists,</u> 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) <u>if a security association exists,</u> rewrite the 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 port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter if 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 value saved from the P-Called-Party-ID header of the request;

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

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a target refresh request (including requests relating to an existing dialog where the method is unknown), prior to forwarding the request, the P-CSCF shall:

1) add its own address to the top of the received list of Via header and save the list The P-CSCF Via header entry is built in a format that contains 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 1: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

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

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

- if a PDF exists for the user for which this response is sent, and if a media authorization token is generated by the PDF, (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

NOTE 2: Typically, the first 183 (Session Progress) response contains an SDP answer including one or more "m=" media descriptions, but it is also possible that the response does not contain an SDP answer or the SDP does not include at least an "m=" media description. However, the media authorization token is generated independently of the presence or absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value. The same media authorization token is used until the session is terminated. For further details see 3GPP TS 29.207 [12].

If a PDF 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 PDF over the Go and Gq 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 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:

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

NOTE 2: Typically, the initial INVITE request contains an SDP offer including one or more "m=" media descriptions, but it is also possible that the INVITE request does not contain an SDP offer or the SDP does not include at least an "m= media description. However, the media authorization token is generated independently of the presence or absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value. The same media authorization token is used until the session is terminated. For further details see 3GPP TS 29.207 [12].

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

If a PDF 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 PDF, over the Go and Gq 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 PDF), 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 sending out a CANCEL request 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 interface resources are no longer available for a session (e.g. abort session request from PDF), 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 release that 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) status code;
   - 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) status code;
- 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 Gq interface 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 Gq interface or Gq' interface, that the session has terminated.

5.2.10 Emergency service

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

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

~~The P-CSCF shall inspect the Request URI of all INVITE requests from the UE for known emergency numbers and emergency URIs from these configurable lists. If the P-CSCF detects that the Request-URI of the INVITE request matches one of the numbers in any of these lists, the P-CSCF shall not forward the INVITE request. The P-CSCF shall respond the INVITE request with a 380 (Alternative Service) response.~~

~~In order to determine whether the INVITE request is destined for an emergency centre in the roaming country (i.e. the list of roaming partners' are inspected):~~

~~T~~the P-CSCF shall compare the MCC and the MNC fields in the received in the P-Access-Network-Info header of the INVITE request against its own MCC and MNC codes.

~~The P-CSCF shall include in the 380 (Alternative Service) response a Content-Type header field with the value set to associated MIME type of the 3GPP IMS XML body as described in subclause 7.6.1.~~

~~The P-CSCF shall include in the 3GPP IMS XML body:~~

~~a) an <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.~~

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: 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 request for a dialog or standalone transaction or an unknown method is destined for a PSAP.

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

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: <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: 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.

5.2.10.2 General treatment for all dialogs and standalone transactions excluding the REGISTER method - from an unregistered user

If the P-CSCF receives an initial request for a dialog or standalone transaction, or an unknown method for an unregistered user on the IP address and the unprotected port advertised to the UE during the P-CSCF discovery or the SIP default port, the P-CSCF shall inspect the Request URI independent of values of possible entries in the received Route headers for known emergency service identifiers, i.e. emergency numbers and the emergency service URN from the 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 380 (Alternative Service) response to the UE, as specified in subclause 5.2.10.1.

If the P-CSCF detects that the Request-URI of the initial request for a dialog or standalone transaction, or 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" in accordance with draft-ietf-ecrit-service-urn [69]. An additional sub-service type can be added if information on the type of emergency service is known. The entry in the Request-URI that the P-CSCF includes may either be:

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

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

2) select an E-CSCF and add the URI of the selected E-CSCF to the topmost Route header; and

NOTE: How the list of E-CSCF is obtained by the P-CSCF is implementation dependent.

3) execute the procedure described in subclause 5.2.6.3 dealing with the procedure when the P-CSCF receives an initial request from the UE and subclause 5.2.7.2 except for:

   - verifying the preloaded route against the received Service-Route header;

   - removing the P-Preferred-Identity header; and

   - inserting a P-Asserted-Identity header.

When the P-CSCF receives any 1xx or 2xx response to the above requests, the P-CSCF shall execute the appropriate procedure for the type of request described in subclause 5.2.6.3, except that the P-CSCF may rewrite the port number of its own Record-Route entry to an unprotected port where the P-CSCF wants to receive the subsequent incoming requests from the UE belonging to this dialog.

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

When the P-CSCF receives a target refresh request from the UE for a dialog, the P-CSCF shall execute the procedure described in step 1) to 5), in paragraph of subclause 5.2.6.3 describing the procedure when the P-CSCF receives a target refresh request.

When the P-CSCF receives from the UE subsequent requests other than a target refresh request (including requests relating to an existing dialog where the method is unknown), the P-CSCF shall execute the procedure described in step 1) to 4), in the paragraph of subclause 5.2.6.3 describing the procedure when the P-CSCF receives a subsequent request.

When the P-CSCF receives any 1xx or 2xx response to the above requests, the P-CSCF shall execute the appropriate procedure for the type of request described in subclause 5.2.6.3.

When the P-CSCF receives, destined for the UE, a target refresh request for a dialog, prior to forwarding the request, the P-CSCF shall execute the procedure described in step 3, the paragraph of subclause 5.2.6.4 describing when the P-CSCF receives a target refresh request.

When the P-CSCF receives a 1xx or 2xx response to the above request the P-CSCF shall execute the procedure described in step 1) to 3) in the paragraph of subclause 5.2.6.4 describing when the P-CSCF receives 1xx or 2xx response to a target request.

When the P-CSCF receives any other response to the above request the P-CSCF shall execute the procedure described in step 1) to 2) in the paragraph of subclause 5.2.6.4 describing when the P-CSCF receives any other response to a target request.

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a target refresh request (including requests relating to an existing dialog where the method is unknown), prior to forwarding the request, the P-CSCF shall execute the procedure described in steps 2 and 3 of subclause 5.2.6.4 describing when a P-CSCF receives a subsequent request.

When the P-CSCF receives any other response to the above request the P-CSCF shall execute the procedure described in step 1 in the paragraph of subclause 5.2.6.4 describing when the P-CSCF receives any other response to a subsequent request.

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

If the P-CSCF receives an initial request for a dialog, or a standalone transaction, or an unknown method, for a registered user ~~over the security association 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.

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

2) 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.

5.2.10.4 General treatment for all dialogs and standalone transactions excluding the REGISTER method - non-emergency registration

If the P-CSCF receives an initial request for a dialog, or a standalone transaction, or an unknown method, for a registered user 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 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 2, 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.

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

2) the P-CSCF shall:

   - if the public user identity included in the P-Preferred-Identity header matches one of the registered public user identities, remove the P-Preferred-Identity header from the received request and insert a P-Asserted-Identity header that includes the 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 public user identity. If the tel URI associated with one of the registered public user identities 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 a public user identity associated with the tel URI;

   - 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.

5.2.10.5 Abnormal cases

If the IM CN subsystem to where the P-CSCF belongs to is not capable to handle emergency sessions or due to local policy does not handle emergency sessions or only handles certain type of emergency session request, the P-CSCF shall not forward the INVITE request. The P-CSCF shall respond to the INVITE request with a 380 (Alternative Service) response, see subclause 5.2.10.1.

NOTE: Some networks only allow session requests which are in accordance with draft-ietf-ecrit-service-urn [69].

5.4.1.1 Introduction

The S-CSCF 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-CSCF procedures for SIP registration that do not relate to emergency. All registration requests are first screened according to the procedures of subclause 5.4.8.2 to see if they do relate to an emergency public user identity.

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

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

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

The S-CSCF 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-CSCF shall perform the initial registration procedures with IMS-AKA authentication described in section 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-CSCF shall perform the initial registration procedures as described in section 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-CSCF receives a correct authentication challenge response in a REGISTER request that is sent integrity protected.

NOTE 2: A REGISTER with Expires header value equal to zero should always be received protected. However, it is possible that in error conditions a REGISTER with Expires header value equal to zero may be received unprotected. In that instance the procedures below will be applied.

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 an already registered public user identity linked to the same private user identity but with a new contact information (e.g. a user roams to a different network without de-registering the previous one), the S-CSCF shall:

1) perform the procedure for receipt of a REGISTER request ~~without an "integrity-protected" parameter, or~~ with the "integrity-protected" parameter in the Authorization header set to "no"', for the received public user identity; and

2) if the authentication has been successful and if the previous registration has not expired, the S-CSCF shall perform the network initiated deregistration procedure only for the previous contact information as described in subclause 5.4.1.5.

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-CSCF shall:

1) identify the user by the public user identity as received in the To header and the private user identity as received in the username field in the Authorization header of the REGISTER request;

2) check if the P-Visited-Network 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-CSCF has performed the Cx Multimedia Authentication procedure with the HSS, as described in 3GPP TS 29.228 [14], the S-CSCF shall select an authentication vector as described in 3GPP TS 33.203 [19].

   Prior to performing Cx Multimedia Authentication procedure with the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14];

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

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

4) store the icid 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:

   - the home network identification in the realm field;
   - the RAND and AUTN parameters and optional server specific data for the UE in the nonce field;
   - the security mechanism, which is AKAv1-MD5, in the algorithm field;
   - the IK (Integrity Key) parameter for the P-CSCF in the ik field (see subclause 7.2A.1); and
   - the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2A.1);

6) store the RAND parameter used in the 401 (Unauthorized) response for future use in case of a resynchronisation. If a stored RAND already exists in the S-CSCF, the S-CSCF shall overwrite the stored RAND with the RAND used in the most recent 401 (Unauthorized) response;

7) send the so generated 401 (Unauthorized) response towards the UE; and

8) start timer reg-await-auth which guards the receipt of the next REGISTER request.

If the received REGISTER request indicates that the challenge sent previously by the S-CSCF to the UE was deemed to be invalid by the UE, the S-CSCF shall stop the timer reg-await-auth and proceed as described in the subclause 5.4.1.2.3.

5.4.1.2A 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 an already registered public user identity linked to the same private user identity but with a new contact information, the S-CSCF 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 if the previous registration has not expired, the S-CSCF shall perform the network initiated deregistration procedure only for the previous contact information as described in subclause 5.4.1.5.

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-CSCF 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-CSCF 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-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14];

NOTE 1: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

NOTE 2: When passing its SIP URI to the HSS, the S-CSCF may include in its SIP URI the transport protocol and the port number where it wants to be contacted.

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

5) In the particular case where the S-CSCF 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-CSCF 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-CSCF 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-CSCF 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-CSCF, the S-CSCF shall:

- reject the REGISTER request with a 423 (Interval Too Brief) response, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

On receiving a failure response to one of the third-party REGISTER requests, based on the information in the Filter Criteria the S-CSCF may:

- abort sending third-party REGISTER requests; and

- initiate network-initiated deregistration procedure.

If the Filter Criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the AS, the S-CSCF shall not initiate network-initiated deregistration procedure.

In the case that the REGISTER request from the UE contains more than one SIP URIs as Contact header entries, the S-CSCF shall store:

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

- an entry decided by the S-CSCF 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-CSCF receives a REGISTER request with the Expires header field containing the value zero, the S-CSCF shall:

- check whether any of the following conditions apply. The S-CSCF 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-CSCF shall only proceed with the following steps if the "integrity-protected" parameter is set to "yes";~~

- release each multimedia session that includes this user, where the session was initiated by this UE with the public user identity found in the P-Asserted-Identity header field or with one of the implicitly registered public user identities by applying the steps listed in subclause 5.4.5.1.2;
- 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-CSCF will only remove the contact address that was registered by this UE;
- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria 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-CSCF may consider the UE and P-CSCF subscriptions to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

If the Authorization header of the REGISTER request ~~did not contain an "integrity-protected" parameter, or~~contained the "integrity-protected" parameter set to the value "no", the S-CSCF shall apply the procedures described in subclause 5.4.1.2.1.

On completion of the above procedures in this subclause and of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.228 [14], for one or more public user identities, the S-CSCF shall update or remove those public user identities, their registration state and the associated service profiles from the local data (based on operators' policy the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber).

5.4.1.6 Network-initiated reauthentication

The S-CSCF may request a subscriber to reauthenticate at any time, based on a number of possible operator settable triggers as described in subclause 5.4.1.2 or subclause 5.4.1.2A.

If the S-CSCF is informed that a private user identity needs to be re-authenticated, the S-CSCF shall generate a NOTIFY request on all dialogs which have been established due to subscription to the reg event package of that user. For each NOTIFY request the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;
2) set the Event header to the "reg" value;
3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns:
   a) set the <uri> sub-element inside the <contact> sub-element of each <registration> element to the contact address provided by the UE;
   b) set the aor attribute within each <registration> element to one public user identity;
   c) set the state attribute within each <registration> element to "active";
   d) set the state attribute within each <contact> element to "active";
   e) set the event attribute within each <contact> element that was registered by this UE to "shortened"; and

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

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

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

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

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

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

When generating the NOTIFY request, the S-CSCF shall shorten the validity of all registration lifetimes associated with this private user identity to an operator defined value that will allow the user to be re-authenticated.

5.4.1.7 Notification of Application Servers about registration status

During registration, the S-CSCF shall include a P-Access-Network-Info header (as received in the REGISTER request from the UE) in the 3rd-party REGISTER sent towards the ASs, if the AS is part of the trust domain. If the AS is not part of the trust domain, the S-CSCF shall not include any P-Access-Network-Info header. The S-CSCF shall not include a P-Access-Network-Info header in any responses to the REGISTER request.

If the registration procedure described in subclauses 5.4.1.2, 5.4.1.2A, 5.4.1.4 or 5.4.1.5 (as appropriate) was successful, the S-CSCF shall send a third-party REGISTER request to each AS with the following information:

a) the Request-URI, which shall contain the AS's SIP URI;

b) the From header, which shall contain the S-CSCF's SIP URI;

c) the To header, which shall contain a non-barred public user identity. 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, as configured by the operator;

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

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

f) for user-initiated deregistration (subclause 5.4.1.4) and network-initiated deregistration (subclause 5.4.1.5), the 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-CSCF 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-CSCF shall set the value of the Content-Type header to include the MIME type specified in subclause 7.6;

h) for initial registration and user-initiated reregistration, the P-Charging-Vector header, which shall contain the same icid parameter that the S-CSCF received in the original REGISTER request from the UE. The S-CSCF 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;

i) for initial registration and user-initiated reregistration, a P-Charging-Function-Addresses header, which shall contain the values received from the HSS if the message is forwarded within the S-CSCF home network.

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

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

- if the default handling defined in the filter criteria indicates the value "SESSION_TERMINATED" as specified in 3GPP TS 29.228 [14], the S-CSCF 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-CSCF receives from the served user or from a PSI an initial request for a dialog or a request for a standalone transaction, prior to forwarding the request, the S-CSCF shall:

Editor's Note: It needs to be stated, that the S-CSCF will only perform the following steps if the request was received from a trusted entity, e.g. an entity within the trust domain.

1) determine whether the request contains a barred public user identity in the P-Asserted-Identity header field of the request or not. In case the said header field contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. The response may include a Warning header containing the warn-code 399. Otherwise, continue with the rest of the steps;

NOTE 1: If the P-Asserted-Identity header field contains a barred public user identity, then the message has been received, either directly or indirectly, from a non-compliant entity which should have had generated the content with a non-barred public user identity.

2) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request;

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

4) check whether the initial request matches the next unexecuted initial filter criteria based on a public user identity in the P-Asserted-Identity header in the priority order as described in 3GPP TS 23.218 [5], and if it does, the S-CSCF shall:

   a) insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4; and

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

NOTE 2: Depending on the result of processing the filter criteria the S-CSCF might contact one or more AS(s) before processing the outgoing Request URI.

5) if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. Optionally, the S-CSCF may generate a new, globally unique icid and insert the new value in the icid parameter of the P-Charging-Vector header when forwarding the message. If the S-CSCF creates a new icid, then it is responsible for maintaining the two icid values in the subsequent messaging;

6) if there is no original dialog identifier present in the topmost Route header of the incoming request insert an orig-ioi parameter into the P-Charging-Vector header. The S-CSCF shall set the orig-ioi parameter to a value that identifies the sending network. The S-CSCF shall not include the term-ioi parameter;

7) if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

8) if there is no original dialog identifier present in the topmost Route header of the incoming request and if the S-CSCF has knowledge of an associated tel-URI for a SIP URI contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;

9) if the request is not forwarded to an AS and if the outgoing Request-URI is a tel URI, the S-CSCF shall translate the E.164 address (see RFC 3966 [22]) to a globally routeable SIP URI using an ENUM/DNS translation mechanism with the format specified in RFC 3761 24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g. a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator. If the request is forwarded, the S-CSCF shall remove the access-network-charging-info parameter from the P-Charging-Vector header prior to forwarding the message. If the outgoing Request-URI is a pres URI or an im URI, the S-CSCF shall forward the request as specified in RFC 3861 [63]. In this case, the S-CSCF shall not modify the received Request-URI;

10) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header if present, otherwise based on the Request-URI. 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 request shall be forwarded to the destination address via an IBCF in the same network;

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

12) in case of an initial request for a dialog originated from a served user, either:

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

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

NOTE 3: For requests originated from a PSI the S-CSCF can decide whether to record-route or not.

Editor's Note: It needs to be clarified how the S-CSCF decides whether to put its address into the Record-Route header in the case of handling a request that originates from a PSI. It might be part of the operators policy.

13) 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;

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

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

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

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

NOTE 4: When the S-CSCF does not have the user profile, before executing the actions as listed above, it initiates the S-CSCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informs the HSS that the user is unregistered. The S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14].

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

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

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

If the S-CSCF receives any final response from the AS, 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-CSCF receives any response to the above request, the S-CSCF may:

1) apply any privacy required by RFC 3323 [33] and RFC 3325 [34] to the P-Asserted-Identity header, although the S-CSCF 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 5: The P-Asserted-Identity header would normally only be expected in 1xx or 2xx responses.

NOTE 6: 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 6a: 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 [2].

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

When the S-CSCF receives any 1xx or 2xx response to the initial request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response in order to be able to release the session if needed.

When the S-CSCF, upon sending an initial INVITE request that includes an IP address in the SDP offer (in "c=" parameter), receives an error response indicating that the IP address type is not supported, (e.g., the S-CSCF receives the 488 (Not Acceptable Here) with 301 Warning header indicating "incompatible network address format"), the S-CSCF shall either:

- fork the initial INVITE request to the IBCF; or

- process the error response and forward it using the Via header.

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

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

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

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

4) in case the request is routed towards the destination user (Request-URI) or 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-CSCF receives any 1xx or 2xx response to the target refresh request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed.

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

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

2) in case the request is routed towards the destination user (Request-URI) or 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-CSCF shall not recurse on 3xx responses.

5.4.3.3 Requests terminated at the served user

When the S-CSCF 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-CSCF shall:

1) void;

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

3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request.

   - If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request.

   - If not present, it indicates that the request is visiting the S-CSCF for the first time, and in this case:

     - determine whether the request contains a barred public user identity in the Request-URI of the request or not. In case the Request URI contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 404 (Not Found) response. Otherwise, continue with the rest of the steps;

     - the S-CSCF shall save the Request-URI from the request;

4) if there is a original dialog identifier present in the topmost Route header of the incoming request check whether the Request-URI equals to the saved value of the Request-URI. If there is no match, then:

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

   b) forward the request based on the topmost Route header or if not available forward the request based on the Request-URI (routing based on Request-URI is specified starting step 9 from subclause 5.4.3.2) and skip the following steps.

   If there is a match, then check whether the initial request matches the next unexecuted initial filter criteria in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

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

5) if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header field, if not present, populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

6) if there 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;

7) if there is 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. The orig-ioi parameter identifies the sending network of the request message. The orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS;

8) if necessary perform the caller preferences to callee capabilities matching according to RFC 3841 [56B];

9) in case there are no Route headers in the request, then determine, from the destination public user identity, the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2. Furthermore, the S-CSCF shall:

   a) build the Route header field with the values determined in the previous step;

   b) determine, from the destination public user identity, the saved Contact URI where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2. If there is more than one contact address saved for the destination public user identity, the S-CSCF shall:

      - 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-CSCF 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-CSCF 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-CSCF shall decide locally whether to fork or perform sequential search among the contact addresses;

   c) build a Request-URI with the contents of the saved Contact URI determined in the previous step; and

   d) insert a P-Called-Party-ID SIP header field including the Request-URI received in the request;

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

11) 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-CSCF 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 2: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

NOTE 2a: 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 [3].

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

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

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

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

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

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

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

If the S-CSCF receives any final response from the AS, 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-CSCF receives, destined for an unregistered user, an initial request for a dialog or a request for a standalone transaction, the S-CSCF shall:

1) if the S-CSCF does not have the user profile, then initiate the S-CSCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informing the HSS that the user is unregistered, but this S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14];

2) execute the procedures described in the steps 1, 2 and 3 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction); and

3) execute the procedure described in step 4, 5, 6, 7, 8, 10, 12 and 13 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

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

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

2) insert a term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi;

3) in the case where the S-CSCF has knowledge of an associated tel URI for a SIP URI contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel URI; and

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

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

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

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

2) insert a term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi.

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

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

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

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

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

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

1) if the response corresponds to an INVITE request, save the Record-Route and Contact header field values in the response such that the S-CSCF is able to release the session if needed; and

2) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header and the access-network-charging-info parameter in the P-Charging-Vector header.

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

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

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

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

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

5.4.8 Emergency service

5.4.8.1 General

S-CSCF shall handle the emergency registration as per the needs of the normal registration.

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

5.4.8.2 Initial emergency registration or user-initiated emergency reregistration

When the S-CSCF receives a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no" and the To header includes an emergency public user identity the S-CSCF shall perform the actions as specified in subclause 5.4.1.2.1 with the following additions:

- if the emergency user identity is linked to a private user identity that has a registered emergency public user identity but with a new contact address, and the authentication has been successful and if the previous emergency registration has not expired, the S-CSCF shall delete the previous contact information. Contacts related to non-emergency registration shall not be deregistered.

When the S-CSCF receives a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall identify the user by the emergency public user identity as received in the To header and the private user identity as received in the Authorization header of the REGISTER request the S-CSCF shall perform the actions as specified in subclause 5.4.1.2.2 with the following additions:

- the S-CSCF shall not include a Service-Route in the 200 (OK) to the REGISTER request;

- store the Path header and the contact information including all header parameters contained in the Contact header. The S-CSCF shall use the Path header and the contact information obtained during the emergency registration to build a preloaded Route header values for the emergency dialogs destined for the UE; and

NOTE 1: The Path header and contact information used for the emergency dialogs destined for the UE and obtained during the emergency registration can be different than the Path header used for the non-emergency communication and obtained during the non-emergency registration.

NOTE 2: If the previous emergency registration with different contact information or emergency Path header has not expired, the S-CSCF will not perform the network initiated deregistration procedure for the previous emergency registration, but will let it expire.

- the S-CSCF shall not send any third-party REGISTER requests to any AS.

5.4.8.3 User-initiated emergency deregistration

When S-CSCF receives a REGISTER request with the Expires header field containing the value zero and the To header includes an emergency public user identity as specified in 3GPP TS 23.003 [3], the S-CSCF shall reject the REGISTER request by sending a 501 (Not Implemented) response.

NOTE: The UE cannot deregister its emergency public user identity.

5.4.8.4 Network-initiated emergency deregistration

The S-CSCF shall not perform a network-initiated emergency deregistration for an emergency public user identity.

5.4.8.5 Network-initiated emergency reauthentication

The S-CSCF shall not reauthenticate an emergency public user identity.

5.4.8.6 Subscription to the event providing registration state

If a S-CSCF receives a SUBSCRIBE request addressed to S-CSCF containing the Event header with the reg event package with a emergency public user identity in the To header, the S-CSCF shall reject the SUBSCRIBE request for the reg-event package by sending a 489 (Bad Event) response.

5.4.8.7 Notification of the registration state

The S-CSCF shall not send a NOTIFY request addressed to an emergency public user identity regarding its subscription state.

5.6.2 Session initiation transaction

When the BGCF receives an INVITE request, the BGCF shall forward the request either:

- to an MGCF within its own network; ~~or~~
- to another network containing an MGCF; or
- where the request is for another network, to an IBCF in its own network, if local policy requires IBCF capabilities towards another network.

The BGCF need not Record-Route the INVITE request. While the next entity may be a MGCF acting as a UA, the BGCF shall not apply the procedures of RFC 3323 [33] relating to privacy. The BGCF shall store the values received in the P-Charging-Function-Addresses header. The BGCF shall store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header.

NOTE 1: The means by which the decision is made to forward to an MGCF or to another network is outside the scope of the present document, but may be by means of a lookup to an external database, or may be by data held internally to the BGCF.

When the BGCF receives an INVITE request, if the BGCF inserts its own Record-Route header, the BGCF may require the periodic refreshment of the session to avoid hung states in the BGCF. If the BGCF requires the session to be refreshed, it shall apply the procedures described in RFC 4028 [58] clause 8.

NOTE 2: 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.

5.10.1 General

As specified in 3GPP TS 23.228 [7] border control functions may be applied between two IM CN subsystems or between an IM CN subsystem and other SIP-based multimedia networks based on operator preference. The IBCF may act both as an entry point and as an exit point for a network. If it processes a SIP request received from other network it functions as an entry point (see subclause 5.10.2) and it acts as an exit point whenever it processes a SIP request sent to other network (see subclause 5.10.3).

The functionalities of the IBCF include:

- network configuration hiding (see subclause 5.10.4);
- application level gateway (see subclause 5.10.5);
- transport plane control, i.e. QoS control;
- screening of SIP signalling (see subclause 5.10.6); and
- inclusion of an IWF if appropriate.

NOTE: The functionalities performed by the IBCF are configured by the operator, and it is network specific.

Editor's Note: It is FFS, whether a separate subclause needed to describe the transport plane control, or it will be added to application level gateway description (as in IBCF the QoS control functionality requires IMS-ALG functionality).

5.10.2.2 Initial requests

Upon receipt of any request, except the REGISTER method, the IBCF shall:

1) if the request is an INVITE request, respond with a 100 (Trying) provisional response;
2) if the request is an INVITE request and the IBCF is configured to perform application level gateway and/or transport plane control functionalities, save the Contact, CSeq and Record-Route header field values received in the request such that the IBCF is able to release the session if needed;
3) if network topology hiding is required, apply the procedures as described in subclause 5.10.4;
4) if screening of SIP signalling is required, apply the procedures as described in 5.10.6;
5) if IBCF processes a request without a pre-defined route (e.g. the subscription to reg event package originated by the P-CSCF), then IBCF shall select an entry point of the home network and forward the request to that entry point;

NOTE 1: The list of the entry points can be either obtained as specified in RFC 3263 [27A] or provisioned in the IBCF. The entry point can be an IBCF or an I-CSCF.

6) store the values from the P-Charging-Function-Addresses header, if present; and
7) remove the P-Charging-Vector and the P-Charging-Function-Addresses headers, if present, prior to forwarding the message.

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

NOTE 2: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

When the IBCF receives a response to the initial request and network topology hiding is required, then the IBCF shall apply the procedures as described in subclause 5.10.4.

When the IBCF receives a response to the initial request and screening of SIP signalling is applied, then the IBCF shall apply the procedures as described in 5.10.6.

5.10.2.3 Subsequent requests

Upon receipt of any request, except the REGISTER method, the IBCF shall:

1) if the request is an INVITE request, respond with a 100 (Trying) provisional response;

2) if the request is a target refresh request and the IBCF is configured to perform application level gateway and/or transport plane control functionalities, save the Contact and CSeq header field values received in the request such that the IBCF is able to release the session if needed;

3) if the subsequent request is other than a target refresh request (including requests relating to an existing dialog where the method is unknown) and the IBCF is configured to perform application level gateway and/or transport plane control functionalities, save the Contact and CSeq header field values received in the request such that the IBCF is able to release the session if needed;

4) if network topology hiding is required, apply the procedures as described in subclause 5.10.4; and

5) if screening of SIP signalling is required, then apply the procedures as described in 5.10.6

When the IBCF receives a response to the subsequent request and network topology hiding is required, then the IBCF shall apply the procedures as described in subclause 5.10.4.

When the IBCF receives a response to the subsequent request and screening of SIP signalling is required, then the IBCF shall apply the procedures as described in 5.10.6.

5.10.3.1 Registration

When IBCF receives a REGISTER request, the IBCF shall:

1) verify if it arrived from a trusted domain or not. If the request arrived from an untrusted domain, respond with 403 (Forbidden) response;

NOTE 1: The IBCF can find out whether the request arrived from a trusted domain or not, from the procedures described in 3GPP TS 33.210 [19A].

2) if network topology hiding, or screening of SIP signalling is required or IBCF is configured to perform application level gateway and/or transport plane control functionalities, add its own routeable SIP URI to the top of the Path header; and

NOTE 2: The IBCF can include in the inserted SIP URI an indicator that identifies the direction of subsequent requests received by the IBCF i.e., from the S-CSCF towards the P-CSCF, to identify the UE-terminating case. The IBCF can encode this indicator in different ways, such as, e.g., a unique parameter in the URI, a character string in the username part of the URI, or a dedicated port number in the URI.

NOTE 3: Any subsequent request that includes the direction indicator (in the Route header) or arrives at the dedicated port number, indicates that the request was sent by the S-CSCF towards the P-CSCF.

3) If IBCF is co-located with an I-CSCF, or it has a preconfigured I-CSCF to be contacted, forward the request to that I-CSCF. Otherwise select an I-CSCF and forward the request to that I-CSCF.

Editor's Note: It is FFS, whether for an IBCF in the home network it is useful to allow the I-CSCF selection. It adds extra flexibility to the network topology, but adds extra complexity as well. The possible two level re-selection can be too much for the SIP timers.

If the selected I-CSCF:

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

the IBCF shall select a new I-CSCF and forward the original REGISTER request.

NOTE 4: The list of the I-CSCFs can be either obtained as specified in RFC 3263 [27A] or provisioned in the IBCF.

If the IBCF fails to forward the REGISTER request to any I-CSCF, the IBCF shall send back a 408 (Request Timeout) response or 504 (Server Time-Out) response towards the P-CSCF, in accordance with the procedures in RFC 3261 [26].

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 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, 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 misoperation of the IM CN subsystem:

- Authorization; and
- WWW-Authenticate.

Where the IBCF appears in the path between the UE and the S-CSCF, some 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: Where operator requirements can be achieved by configuration hiding, then these procedures can be used in preference to screening.

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 annexes F and G.

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), and possibly record the event in the CDR.

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 possibly record the event in the CDR.

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), and possibly record the event in the CDR.

5.11 Procedures at the E-CSCF

5.11.1 General

The PSAP may either be directly connected to the IM CN subsystem or via the PSTN.

The E-CSCF retrieves a PSAP URI, based on the location of the UE. The PSAP URI can be retrieved from LRF or from local configuration. The PSAP address will either point to a PSAP connected to the IM CN subsystem or to a PSAP connected to the PSTN.

If the E-CSCF fails to select a PSAP based on the received location information contained in an INVITE request, the E-CSCF can interrogate the LRF in order to retrieve location information.

NOTE: The protocol used between an E-CSCF and an LRF and between an E-CSCF and an external server is not specified in this version of the specification.

5.11.2 UE originating case

The E-CSCF may either forward the call to a PSAP in the IP network or forward the call to a PSAP in the PSTN. In the latter case the call will pass a BGCF and a MGCF before entering the PSTN.

Upon receipt of an initial request for a dialog, or a standalone transaction, or an unknown method including a Request-URI with an emergency service URN in accordance with draft-ietf-ecrit-service-urn [69] or an emergency number the E-CSCF shall:

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

2) if the PSAP is the next hop, store the value of the icid parameter received in the P-Charging-Vector header and remove the received information in the P-Charging-Vector header, else keep the P-Charging-Vector if the next hop is an exit IBCF or a BGCF;

3) if the PSAP is the next hop remove the P-Charging-Function-Addresses headers, if present, else keep the P-Charging-Function-Addresses headers if the next hop is an exit IBCF or an BGCF;

4) if an IBCF or BGCF is the next hop insert a type 2 orig-ioi parameter into the P-Charging-Vector header. The E-CSCF shall set the type 2 orig-ioi parameter to a value that identifies the sending network. The E-CSCF shall not include the term-ioi parameter;

5) get location information as:

- geographical location information received as a location object from a message body with the content type application/pidf+xml in accordance with draft-ietf-sip-location-conveyance [89]; and

- location identifier as derived from the P-Access-Network Network-Info header, if available.

NOTE 1: The E-CSCF can request location information from an LRF. The protocol used to retrieve the location information from the LRF is not specified in this version of the specification.

NOTE 2: As an alternative to retrieve location information from the LRF the E-CSCF can also request location information from an external server. The address to the external server can be received in the Geolocation header as specified in draft-ietf-sip-location-conveyance [89]. The protocol used to retrieve the location information from the external server is not specified in this version of the specification.

6) select, based on location information and optionally type of emergency service:

- a PSAP connected to the IM CN subsystem network and add the PSAP URI to the topmost Route header; or

NOTE 3: The E-CSCF conveys the P-Access-Network-Info header containing the location identifier to the PSAP.

- a PSAP in the PSTN, add the BGCF URI to the topmost Route header and add a PSAP URI in tel URI format to the Request-URI with an entry used in the PSTN/CS domain to address the PSAP;

NOTE 4: The E-CSCF conveys the P-Access-Network-Info header containing the location identifier towards the MGCF. The MGCF can translate the location Information if included in INVITE (i.e. both the geographical location information in PIDF-LO and the location identifier in the P-Access-Network-Info header) into ISUP signalling, see 3GPP TS 29.163 [11B].

NOTE 5: The E-CSCF can request location information and routeing information from the LRF. The E-CSCF can for example send the location identifier to LRF and LRF maps the location identifier into the corresponding geographical location information that LRF sends to E-CSCF. The LRF can invoke an RDF to convert the location information into a proper PSAP/EC URI. Both the location information and the PSAP URI are returned to the E-CSCF.

NOTE 6: The way the E-CSCF determines the next hop address when the PSAP address is a tel URI is implementation dependent.

7) if the E-CSCF receives a reference number from the LRF the E-CSCF shall include the reference number in the P-Asserted-Identity header;

NOTE 7: The reference number is used in the communication between the PSAP and LRF.

8) if due to local policy or if the PSAP requires interconnect functionalities (e.g. PSAP address is of an IP address type other than the IP address type used in the IM CN subsystem), put the address of the IBCF to the topmost route header, in order to forward the request to the PSAP via an IBCF in the same network;

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

10) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the E-CSCF is able to release the session if needed; and

11) route the request based on SIP routeing procedures.

Editor's Note: It needs to be investigated whether the E-CSCF also needs (under specific circumstances) to release an emergency session.

NOTE 8: Depending on local operator policy, the E-CSCF has the capability to reject requests relating to specific methods in accordance with RFC 3261 [26], as an alternative to the functionality described above.

Upon receipt of an initial request for a dialog, a standalone transaction, or an unknown method, that does not include a Request-URI with an emergency service URN or an emergency number, the E-CSCF shall reject the call by sending a 403 (Forbidden) response.

When the E-CSCF receives the request containing the access-network-charging-info parameter in the P-Charging-Vector, the E-CSCF shall store the access-network-charging-info parameter from the P-Charging-Vector header. The E-CSCF shall retain access-network-charging-info parameter in the P-Charging-Vector header.

When the E-CSCF receives any request or response (excluding ACK requests and CANCEL requests and responses) related to a UE-originated dialog or standalone transaction, the E-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message.

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

NOTE 9: Requesting the session to be refreshed requires support by at least the UE or the PSAP or MGCF. This functionality cannot automatically be granted, i.e. at least one of the involved UAs needs to support it in order to make it work.

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

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208 [13].

NOTE 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 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].

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.

When the P-CSCF receives an initial INVITE request for a terminating session setup or a 183 (Session Progress) response to an INVITE request for an originating session setup, the P-CSCF may modify the SDP according to RFC 3524 [54] to indicate to the UE that particular media stream(s) is grouped according to a local policy. The policy is used to determine whether the P-CSCF will request the UE to keep media stream(s) grouped in different IP-CAN bearers and identify the relation between different media streams and IP-CAN bearers (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

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

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

The P-CSCF may inspect, if present, the "b=RS" and "b=RR" lines in order to find out the bandwidth allocation requirements for RTCP.

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 may be additional coding rules for this header depending on the type of IP-CAN, according to access technology specific descriptions.

Editor's Note: The appropriate usage, beyond the existing Release 5 functionality, of the P-Access-Network-Info header is FFS.

Table 7.6A describes 3GPP-specific extensions to the P-Charging-Vector header field defined in RFC 3455 [52].

Table 7.6A: Syntax of extensions to 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 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
access-info            = cgi-3gpp / utran-cell-id-3gpp / dsl-location / np / 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)
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

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" or "IDSL" as appropriate to the radio/xDSL access technology in use;

Editor's Note: A P-CSCF generally may support more than one access network type. Where this information is inserted should be considered, because the end UE may not be aware of the access network type. Also it should be clarified what would be a potential application of the access network type information.

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 set to one of "IEEE-802.11", "IEEE-802.11a", "IEEE-WLAN-802.11b" or "IEEE-802.11g" the access info parameter is set to a null value. This release of this specification does not define values for use in this parameter; and

5) 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 derived from the binding information (IP edge ID, allocated IP address, line ID).~~

Editor's Note: The dsl-location field would need to be structured in a standardized format. This does not necessarily contain Geographic Location Information suitable to locate an emergency situation.

7.6.2 Document Type Definition

The Document Type Definition, according to XML syntax definitions, is defined in table 7.7.

Table 7.7: IM CN subsystem XML body, version 1 DTD

```
<?xml version="1.0" ?>
<!-- Draft DTD for the IMS XML body. -->

<!DOCTYPE ims-3gpp [
    <!-- ims-3gpp element: root element -->

    <!ELEMENT ims-3gpp (
        alternative-service?, service-info?)>
    <!ATTLIST ims-3gpp version CDATA #REQUIRED>

    <!-- service-info element: The transparent data received from HSS for AS -->
    <!ELEMENT service-info              (#CDATA)>

    <!-- alternative-service: alternative-service used in emergency sessions -->
    <!ELEMENT alternative-service   (type, action?, reason)>
    <!ELEMENT type                  (emergency)>
    <!ELEMENT action                (emergency-registration)>
    <!ELEMENT reason                (#PCDATA)>

]>
```

7.6.3 DTD description

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

<ims-3gpp>: This is the root element of the IMS XML body. It shall always be present. The version described in the present document is 1.

<service-info>: the transparent element received from the HSS for a particular trigger point are placed within this optional element.

<alternative-service>: in the present document, the alternative service is used as a response for an attempt to establish an emergency session within the IM CN subsystem. The element describes an alternative service where the call should success. The alternative service is described by the type of service information. A possible reason cause why an alternative service is suggested may be included.

The <alternative-service> element contains a <type> element that indicates the type of alternative service and an <action> element, an optional element.

The <type> element contains only the value "emergency" in the present document.

The <action> element contains only the value "emergency-registration" in the present document.

The <reason> element contains an explanatory text with the reason why the session setup has been redirected. A UE may use this information to give an indication to the user.

9 IP-Connectivity Access Network aspects when connected to the IM CN subsystem

9.2.2 Handling of the IP-CAN

The UE shall ensure that appropriate resources are available for the media flow(s) on the IP-CAN(s) related to a SIP-session. The means to ensure this is dependant on the characteristics for each IP-CAN, and is described separately for each IP-CAN in question.

GPRS is described in annex B. I-WLAN is described in annex D. xDSL is described in annex E. If a particular handling of the IP-CAN is needed for emergency calls, this is described in the annex for each access technology.

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

~~Editor's note: IBCF related changes not added yet~~

NOTE: IBCF and emergency related changes have not been added yet. This will be reflected in future changes in tables e.g. A.3A, A.4 and A.162.

A.1.3 Roles

Table A.2: Roles

Item	Roles	Reference	RFC status	Profile status
1	User agent	[26]	o.1	o.1
2	Proxy	[26]	o.1	o.1
o.1:	It is mandatory to support exactly one of these items.			
NOTE:	For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.			

Table A.3: Roles specific to this profile

Item	Roles	Reference	RFC status	Profile status
1	UE	5.1	n/a	o.1
2	P-CSCF	5.2	n/a	o.1
3	I-CSCF	5.3	n/a	o.1
3A	I-CSCF (THIG)	5.3	n/a	c1
4	S-CSCF	5.4	n/a	o.1
5	BGCF	5.6	n/a	o.1
6	MGCF	5.5	n/a	o.1
7	AS	5.7	n/a	o.1
7A	AS acting as terminating UA, or redirect server	5.7.2	n/a	c2
7B	AS acting as originating UA	5.7.3	n/a	c2
7C	AS acting as a SIP proxy	5.7.4	n/a	c2
7D	AS performing 3rd party call control	5.7.5	n/a	c2
8	MRFC	5.8	n/a	o.1
9	IMS-ALG	5.9	n/a	o.1
11	E-CSCF	5.11	n/a	o.1
c1:	IF A.3/3 THEN o ELSE x - - I-CSCF.			
c2:	IF A.3/7 THEN o.2 ELSE n/a - - AS.			
o.1:	It is mandatory to support exactly one of these items.			
o.2:	It is mandatory to support at least one of these items.			
NOTE:	For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.			

Table A.3A: Roles specific to additional capabilities

Item	Roles	Reference	RFC status	Profile status
1	Presence server	3GPP TS 24.141 [8A]	n/a	c1
2	Presence user agent	3GPP TS 24.141 [8A]	n/a	c2
3	Resource list server	3GPP TS 24.141 [8A]	n/a	c3
4	Watcher	3GPP TS 24.141 [8A]	n/a	c4
11	Conference focus	3GPP TS 24.147 [8B]	n/a	c5
12	Conference participant	3GPP TS 24.147 [8B]	n/a	c6
c1:	IF A.3/7A AND A.3/7B THEN o ELSE n/a - - AS acting as terminating UA, or redirect server and AS acting as originating UA.			
c2:	IF A.3/1 THEN o ELSE n/a - - UE.			
c3:	IF A.3/7A THEN o ELSE n/a - - AS acting as terminating UA, or redirect server.			
c4:	IF A.3/1 OR A.3/7B THEN o ELSE IF A.3/9 THEN m ELSE n/a - - UE or AS acting as originating UA.			
c5:	IF A.3/7D AND A.3/4 AND A.3/8 THEN o ELSE n/a - - AS performing 3rd party call control and S-CSCF and MRFC (note 2).			
c6:	IF A.3/1 OR A.3A/11 THEN o ELSE IF A.3/9 THEN m ELSE n/a - - UE or conference focus.			
NOTE 1:	For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.			
NOTE 2:	The functional split between the MRFC and the conferencing AS is out of scope of this document and they are assumed to be collocated.			

Table A.3B: Roles with respect to access technology

Item	Value used in P-Access-Network-Info header	Reference	RFC status	Profile status
1	3GPP-GERAN	[52] 4.4	o	c1
2	3GPP-UTRAN-FDD	[52] 4.4	o	c1
3	3GPP-UTRAN-TDD	[52] 4.4	o	c1
4	3GPP2-1X	[52] 4.4	o	c1
5	3GPP2-1X-HRPD	[52] 4.4	o	c1
11	IEEE-802.11	[52] 4.4	o	c1
12	IEEE-802.11°	[52] 4.4	o	c1
13	IEEE-802.11b	[52] 4.4	o	c1
14	IEEE-802.11g	[52] 4.4	o	c1
21	ADSL	[52] 4.4	o	c1
22	ADSL2	[52] 4.4	o	c1
23	ADSL2+	[52] 4.4	o	c1
24	RADSL	[52] 4.4	o	c1
25	SDSL	[52] 4.4	o	c1
26	HDSL	[52] 4.4	o	c1
27	HDSL2	[52] 4.4	o	c1
28	G.SHDSL	[52] 4.4	o	c1
29	VDSL	[52] 4.4	o	c1
30	IDSL	[52] 4.4	o	c1
c1:	If A.3/1 OR A.3/2 THEN o.1 ELSE n/a.			
o.1:	It is mandatory to support at least one of these items.			

A.2.1.2 Major capabilities

Table A.4: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
1	client behaviour for registration?	[26] subclause 10.2	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
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	c18
15	the REFER method?	[36]	o	c33
16	integration of resource management and SIP?	[30] [64]	c19	c18
17	the SIP UPDATE method?	[29]	c5	c18
19	SIP extensions for media authorization?	[31]	o	c14
20	SIP specific event notification?	[28]	o	c13
21	the use of NOTIFY to establish a dialog?	[28] 4.2	o	n/a
22	acting as the notifier of event information?	[28]	c2	c15
23	acting as the subscriber to event information?	[28]	c2	c16
24	session initiation protocol extension header field for registering non-adjacent contacts?	[35]	o	c6
25	private extensions to the Session Initiation Protocol (SIP) for network asserted identity within trusted networks?	[34]	o	m
26	a privacy mechanism for the Session Initiation Protocol (SIP)?	[33]	o	m
26A	request of privacy by the inclusion of a Privacy header indicating any privacy option?	[33]	c9	c11
26B	application of privacy based on the received Privacy header?	[33]	c9	n/a
26C	passing on of the Privacy header transparently?	[33]	c9	c12
26D	application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the assistance of intermediaries are obscured?	[33] 5.1	c10	c27
26E	application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs?	[33] 5.2	c10	c27

26F	application of the privacy option "user" such that user level privacy functions are provided by the network?	[33] 5.3	c10	c27
26G	application of the privacy option "id" such that privacy of the network asserted identity is provided by the network?	[34] 7	c10	n/a
26H	application of the privacy option "history" such that privacy of the History-Info header is provided by the network?	[66] 7.2	c37	c37
27	a messaging mechanism for the Session Initiation Protocol (SIP)?	[50]	o	c7
28	session initiation protocol extension header field for service route discovery during registration?	[38]	o	c17
29	compressing the session initiation protocol?	[55]	o	c8
30	private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP)?	[52]	o	m
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)
45	the Session Initiation Protocol (SIP) "Join" header?	[61]	c19	c19 (note 1)
46	the callee capabilities?	[62]	o	c35
47	an extension to the session initiation protocol for request history information?	[66]	o	o
48	Rejecting anonymous requests in the Session Initiation Protocol (SIP)	[67]	o	o
49	session initiation protocol URIs for applications such as voicemail and interactive voice response	[68]	o	o

52	a uniform resource name for services	[69]	n/a	c39

c2: IF A.4/20 THEN o.1 ELSE n/a - - SIP specific event notification extension.
c3: IF A.3/1 OR A.3/4 THEN m ELSE n/a - - UE or S-CSCF functional entity.
c4: IF A.3/4 THEN m ELSE IF A.3/7 THEN o ELSE n/a - - S-CSCF or AS functional entity.
c5: IF A.4/16 THEN m ELSE o - - integration of resource management and SIP extension.
c6: IF A.3/4 OR A.3/1 THEN m ELSE n/a. - - S-CSCF or UE.
c7: IF A.3/1 OR A.3/4 OR A.3/7A OR A.3/7B OR A.3/7D OR A.3/9 THEN m ELSE n/a - - UA or S-CSCF or AS acting as terminating UA or AS acting as originating UA or AS performing 3rd party call control or 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.3/9 THEN m ELSE n/a - - UE or MGCF, 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.3/9 THEN m ELSE o - - UE or S-CSCF or IMS-ALG.
c14: IF A.3/1 AND (A.3B/1 OR A.3B/2 OR A.3B/3 OR A.3B/4 OR A.3B/5) THEN m ELSE n/a – UE with appropriate access technology
c15: IF A.4/20 AND (A.3/4 OR A.3/9) THEN m ELSE o – SIP specific event notification extensions and S-CSCF, IMS-ALG .
c16: IF A.4/20 AND (A.3/1 OR A.3/2 OR A.3/9) THEN m ELSE o - - SIP specific event notification extension and UE or P-CSCF or IMS-ALG.
c17: IF A.3/1 or A.3/4 THEN m ELSE n/a - - UE or S-CSCF
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-CSCF or UA.
c23: IF A.4/30 AND A.3/1 THEN o ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE.
c24: IF A.4/30 AND A.3/4) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and S-CSCF.
c25: IF A.4/30 AND (A.3/1 OR A.3/4 OR A.3/7A OR A.3/7D OR A.3/9) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and UE, S-CSCF or AS acting as terminating UA or AS acting as third-party call controller, 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.3/11 OR A.3/12 OR A.3/9 OR A.4/44 THEN m ELSE o - - conference focus or conference participant or IMS-ALG or the Session Initiation Protocol (SIP) "Replaces" header.
c34: IF A.4/44 OR A.4/45 OR A.3/9 THEN m ELSE n/a - - the Session Initiation Protocol (SIP) "Replaces" header or the Session Initiation Protocol (SIP) "Join" header or IMS-ALG.
c35: IF A.3/4 OR A.3/9 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-CSCF or IMS-ALG functional entities, 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) THEN m ELSE IF A.4/2B THEN o ELSE n/a - - initiating sessions, conference focus, conference participant
c39: IF A.3/1 THEN m ELSE n/a - - UE.

o.1: At least one of these capabilities is supported.
o.2: At least one of these capabilities is supported.
o.3: At least one of these capabilities is supported.
o.4: At least one of these capabilities is supported.
o.5: At least one of these capabilities is supported.

NOTE 1: At the MGCF, the interworking specifications do not support a handling of the header associated with this extension.

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
2	refer package?	[36] 3	c13	c13	[36] 3	c13	c13
3	presence package?	[74] 6	c1	c5	[74] 6	c2	c6
4	eventlist with underlying presence package?	[75], [74] 6	c1	c7	[75], [74] 6	c2	c8
5	presence.winfo template-package?	[72] 4	c1	c9	[72] 4	c2	c10
6	sip-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

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-CSCF.
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.

A.2.1.4.1 Status-codes

Table A.6: Supported status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	100 (Trying)	[26] 21.1.1	n/a	n/a	[26] 21.1.1	c11	c11
101	1xx response	[26] 21.1	p21	p21	[26] 21.1	p21	p21
2	180 (Ringing)	[26] 21.1.2	c2	c2	[26] 21.1.2	c1	c1
3	181 (Call Is Being Forwarded)	[26] 21.1.3	c2	c2	[26] 21.1.3	c1	c1
4	182 (Queued)	[26] 21.1.4	c2	c2	[26] 21.1.4	c1	c1
5	183 (Session Progress)	[26] 21.1.5	c1	c1	[26] 21.1.5	c1	c1
102	2xx response	[26] 21.2	p22	p22	[26] 21.1	p22	p22
6	200 (OK)	[26] 21.2.1	m	m	[26] 21.2.1	m	m
7	202 (Accepted)	[28] 8.3.1	c3	c3	[28] 8.3.1	c3	c3
103	3xx response	[26] 21.3	p23	p23	[26] 21.1	p23	p23
8	300 (Multiple Choices)	[26] 21.3.1			[26] 21.3.1		
9	301 (Moved Permanently)	[26] 21.3.2			[26] 21.3.2		
10	302 (Moved Temporarily)	[26] 21.3.3			[26] 21.3.3		
11	305 (Use Proxy)	[26] 21.3.4			[26] 21.3.4		
12	380 (Alternative Service)	[26] 21.3.5			[26] 21.3.5		
104	4xx response	[26] 21.4	p24	p24	[26] 21.4	p24	p24
13	400 (Bad Request)	[26] 21.4.1	m	m	[26] 21.4.1	m	m
14	401 (Unauthorized)	[26] 21.4.2	o	c12	[26] 21.4.2	m	m
15	402 (Payment Required)	[26] 21.4.3	n/a	n/a	[26] 21.4.3	n/a	n/a
16	403 (Forbidden)	[26] 21.4.4	m	m	[26] 21.4.4	m	m
17	404 (Not Found)	[26] 21.4.5	m	m	[26] 21.4.5	m	m
18	405 (Method Not Allowed)	[26] 21.4.6	m	m	[26] 21.4.6	m	m
19	406 (Not Acceptable)	[26] 21.4.7	m	m	[26] 21.4.7	m	m
20	407 (Proxy Authentication Required)	[26] 21.4.8	o	o	[26] 21.4.8	m	m
21	408 (Request Timeout)	[26] 21.4.9	m	m	[26] 21.4.9	m	m
22	410 (Gone)	[26] 21.4.10	m	m	[26] 21.4.10	m	m
22A	412 (Conditional Request Failed)	[70] 11.2.1	c20	c20	[70] 11.2.1	c20	c20
23	413 (Request Entity Too Large)	[26] 21.4.11	m	m	[26] 21.4.11	m	m
24	414 (Request-URI Too Large)	[26] 21.4.12	m	m	[26] 21.4.12	m	m
25	415 (Unsupported Media Type)	[26] 21.4.13	m	m	[26] 21.4.13	m	m
26	416 (Unsupported URI Scheme)	[26] 21.4.14	m	m	[26] 21.4.14	m	m
27	420 (Bad Extension)	[26] 21.4.15	m	c13	[26] 21.4.15	m	m
28	421 (Extension Required)	[26] 21.4.16	o		[26] 21.4.16	i	i
28A	422 (Session Interval Too Small)	[58] 6	c7	c7	[58] 6	c7	c7
29	423 (Interval Too Brief)	[26] 21.4.17	c4	c4	[26] 21.4.17	m	m
29A	429 (Provide Referrer Identity)	[59] 5	c8	c8	[59] 5	c9	c9
29B	433 (Anonymity Disallowed)	[67] 4	c14	c14	[67] 4	c14	c14
30	480 (Temporarily Unavailable)	[26] 21.4.18	m	m	[26] 21.4.18	m	m
31	481 (Call/Transaction Does Not Exist)	[26] 21.4.19	m	m	[26] 21.4.19	m	m
32	482 (Loop Detected)	[26] 21.4.20	m	m	[26] 21.4.20	m	m
33	483 (Too Many Hops)	[26] 21.4.21	m	m	[26] 21.4.21	m	m
34	484 (Address Incomplete)	[26] 21.4.22	o	o	[26] 21.4.22	m	m
35	485 (Ambiguous)	[26] 21.4.23	o	o	[26] 21.4.23	m	m
36	486 (Busy Here)	[26] 21.4.24	m	m	[26] 21.4.24	m	m
37	487 (Request Terminated)	[26] 21.4.25	m	m	[26] 21.4.25	m	m
38	488 (Not Acceptable Here)	[26] 21.4.26	m	m	[26] 21.4.26	m	m
39	489 (Bad Event)	[28] 7.3.2	c3	c3	[28] 7.3.2	c3	c3
40	491 (Request Pending)	[26] 21.4.27	m	m	[26] 21.4.27	m	m

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
41	493 (Undecipherable)	[26] 21.4.28	m	m	[26] 21.4.28	m	m
41A	494 (Security Agreement Required)	[48] 2	c5	c5	[48] 2	c6	c6
105	5xx response	[26] 21.5	p25	p25	[26] 21.5	p25	p25
42	500 (Internal Server Error)	[26] 21.5.1	m	m	[26] 21.5.1	m	m
43	501 (Not Implemented)	[26] 21.5.2	m	m	[26] 21.5.2	m	m
44	502 (Bad Gateway)	[26] 21.5.3	o	o	[26] 21.5.3	m	m
45	503 (Service Unavailable)	[26] 21.5.4	m	m	[26] 21.5.4	m	m
46	504 (Server Time-out)	[26] 21.5.5	m	m	[26] 21.5.5	m	m
47	505 (Version not supported)	[26] 21.5.6	m	m	[26] 21.5.6	m	m
48	513 (Message Too Large)	[26] 21.5.7	m	m	[26] 21.5.7	m	m
49	580 (Precondition Failure)	[30] 8			[30] 8		
106	6xx response	[26] 21.6	p26	p26	[26] 21.6	p26	p26
50	600 (Busy Everywhere)	[26] 21.6.1	m	m	[26] 21.6.1	m	m
51	603 (Decline)	[26] 21.6.2	c10	c10	[26] 21.6.2	m	m
52	604 (Does Not Exist Anywhere)	[26] 21.6.3	m	m	[26] 21.6.3	m	m
53	606 (Not Acceptable)	[26] 21.6.4	m	m	[26] 21.6.4	m	m

c1: IF A.5/9 THEN m ELSE n/a - - INVITE response.
c2: IF A.5/9 THEN o ELSE n/a - - INVITE response.
c3: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c4: IF A.5/19 OR A.5/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response.
c5: IF A.4/37 AND A.4/2 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol and registrar.
c6: IF A.4/37 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c7: IF A.4/42 AND (A.5/9 OR A.5/23) THEN m ELSE n/a - - the SIP session timer AND (INVITE response OR UPDATE response).
c8: IF A.4/43 AND A.5/17 THEN o ELSE n/a - - the SIP Referred-By mechanism and REFER response.
c9: IF A.4/43 AND A.5/17 THEN m ELSE n/a - - the SIP Referred-By mechanism and REFER response.
c10: IF A.4/44 THEN m ELSE o - - the Session Initiation Protocol (SIP) "Replaces" header.
c11: IF A.5/9 THE m ELSE n/a - - INVITE response (note 1).
c12: IF A.3/4 THEN m ELSE o - - S-CSCF.
c13: IF A.3/1 OR A.3/2 OR A.3/4 THEN m ELSE o - - UE, P-CSCF, S-CSCF.
c14: IF A.4/48 THEN m ELSE n/a – - rejecting anonymous requests in the session initiation protocol
c20: IF A.4/41 THEN m ELSE n/a - - an event state publication extension to the session initiation protocol.
p21: A.6/2 OR A.6/3 OR A.6/4 OR A.6/5 - - 1xx response.
p22: A.6/6 OR A.6/7 - - 2xx response.
p23: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/13 - - 3xx response.
p24: A.6/14 OR A.6/15 OR A.6/16 OR A.6/17 OR A.6/18 OR A.6/19 OR A.6/20 OR A.6/21 OR A.6/22 OR A.6/22A OR A.6/23 OR A.6/24 OR A.6/25 OR A.6/26 OR A.6/27 OR A.6/28 OR A.6/28A OR A.6/29 OR A.6/29A OR A.6/29B OR A.6/30 OR A.6/31 OR A.6/32 OR A.6/33 OR A.6/34 OR A.6/35 OR A.6/36 OR A.6/436 OR A.6/38 OR A.6/39 OR A.6/40 OR A.6/41 OR A.6/41A. - 4xx response.
p25: A.6/42 OR A.6/43 OR A.6/44 OR A.6/45 OR A.6/46 OR A.6/47 OR A.6/48 OR A.6/49 - - 5xx response
p26: A.6/50 OR A.6/51 OR A.6/52 OR A.6/53 - - 6xx response.

NOTE 1: RFC 3261 [26] gives the status of this header for methods other than INVITE as SHOULD NOT.

A.2.2.2 Major capabilities

Table A.162: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
3	initiate session release?	[26] 16	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
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
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	x
50	caller preferences for the session initiation protocol?	[56B]	c33	c33
50A	the proxy-directive within caller-preferences?	[56B] 9.1	o.4	o.4
50B	the cancel-directive within caller-preferences?	[56B] 9.1	o.4	o.4
50C	the fork-directive within caller-preferences?	[56B] 9.1	o.4	c32
50D	the recurse-directive within caller-preferences?	[56B] 9.1	o.4	o.4
50E	the parallel-directive within caller-preferences?	[56B] 9.1	o.4	c32
50F	the queue-directive within caller-preferences?	[56B] 9.1	o.4	o.4
51	an event state publication extension to the session initiation protocol?	[70]	o	m
52	SIP session timer?	[58]	o	o
53	the SIP Referred-By mechanism?	[59]	o	o
54	the Session Initiation Protocol (SIP) "Replaces" header?	[60]	o	o
55	the Session Initiation Protocol (SIP) "Join" header?	[61]	o	o
56	the callee capabilities?	[62]	o	o
57	an extension to the session initiation protocol for request history information?	[66]	o	o
58	Rejecting anonymous requests in the Session Initiation Protocol (SIP)	[200]	o	o
59	session initiation protocol URIs for applications such as voicemail and interactive voice response	[68]	o	o
60	an SIP Reason header extension for indicating redirection/ communication diversion reasons?	[80]	o	c34
62	a uniform resource name for services	[69]	n/a	c35

c1:	IF A.162/5 THEN o ELSE n/a - - stateful proxy behaviour.
c2:	IF A.3/2 OR A.3/3A OR A.3/4 THEN m ELSE o - - P-CSCF, I-CSCF(THIG) or S-CSCF.
c3:	IF (A.162/7 AND NOT A.162/8) OR (NOT A.162/7 AND A.162/8) THEN m ELSE IF A.162/14 THEN o ELSE n/a - - TLS interworking with non-TLS else proxy insertion.
c4:	IF A.162/23 THEN m ELSE o - - integration of resource management and SIP.
c5:	IF A.162/30 THEN o ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c6:	IF A.3/2 OR A.3/3A THEN m ELSE n/a - - P-CSCF or I-CSCF (THIG).
c7:	IF A.3/2 THEN m ELSE n/a - - P-CSCF.
c8:	IF A.3/2 AND A.162/30 THEN m ELSE n/a - - P-CSCF and extensions to the Session 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-CSCF or AS acting as proxy and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks (note).
c10:	IF A.162/31 THEN 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-CSCF.
c13:	IF A.162/31 AND (A.3/2 OR A.3/3 OR A.3/7C) THEN m ELSE n/a - - P-CSCF OR I-CSCF OR AS acting as a SIP proxy.
c14:	IF A.162/35 THEN o.3 ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP).
c15:	IF A.162/35 AND (A.3/2 OR A.3/3) THEN m 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.
c16:	IF A.162/35 AND (A.3/2 OR A.3/3 OR A.3/4) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF or S-CSCF.
c17:	IF A.162/35 AND (A.3/2 OR A.3/3) THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF or I-CSCF.
c18:	IF A.162/38 THEN o ELSE n/a - - the P-Visited-Network-ID header extension.
c19:	IF A.162/35 AND (A.3/2 OR A.3.3 OR A.3/4 OR A.3/7 THEN m ELSE n/a - - private header extensions to the session initiation protocol for the 3rd-Generation Partnership Project (3GPP) and P-CSCF, I-CSCF, S-CSCF, AS acting as a proxy.
c20:	IF A.162/41 THEN o ELSE n/a - - the P-Access-Network-Info header extension.
c21:	IF A.162/41 AND A.3/2 THEN m ELSE n/a - - the P-Access-Network-Info header extension and P-CSCF.
c22:	IF A.162/41 AND A.3/4 THEN m ELSE n/a - - the P-Access-Network-Info header extension and S-CSCF.
c23:	IF A.162/45 THEN o ELSE n/a - - the P-Charging-Vector header extension.
c24:	IF A.162/45 THEN m ELSE n/a - - the P-Charging-Vector header extension.
c25:	IF A.162/44 THEN o ELSE n/a - - the P-Charging-Function-Addresses header extension.
c26:	IF A.162/44 THEN m ELSE n/a - - the P-Charging-Function Addresses header extension.
c27:	IF A.3/2 OR A.3/4 THEN m ELSE x - - P-CSCF or S-CSCF.
c28:	IF A.3/2 OR A.3/4 OR A.3/6 then m ELSE o - - P-CSCF or S-CSCF of MGCF.
c29:	IF A.3/2 OR A.3/4 OR A.3/6 then o ELSE m - - P-CSCF or S-CSCF of MGCF.
c30:	IF A.3/2 o ELSE i - - P-CSCF.
c31:	IF A.3/4 THEN m ELSE x - - S-CSCF.
c32:	IF A.3/4 THEN m ELSE o.4 - - S-CSCF.
c33:	IF A.162/50A OR A.162/50B OR A.162/50C OR A.162/50D OR A.162/50E OR A.162/50F THEN m ELSE n/a - - support of any directives within caller preferences for the session initiation protocol.
c34	IF A.162/57 THEN m ELSE n/a - - an extension to the session initiation protocol for request history information.
c35:	IF A.3/2 OR A.3/11 THEN m ELSE n/a - - P-CSCF, 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.
NOTE:	An AS acting as a proxy may be outside the trust domain, and therefore not able to support the capability for that reason; in this case it is perfectly reasonable for the header to be passed on transparently, as specified in the PDU parts of the profile.

A.2.2.4.1 Status-codes

Table A.164: Supported-status codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	100 (Trying)	[26] 21.1.1	c1	c1	[26] 21.1.1	c2	c2
101	1xx response	[26] 21.1	p21	p21	[26] 21.1	p21	p21
2	180 (Ringing)	[26] 21.1.2	c3	c3	[26] 21.1.2	c3	c3
3	181 (Call Is Being Forwarded)	[26] 21.1.3	c3	c3	[26] 21.1.3	c3	c3
4	182 (Queued)	[26] 21.1.4	c3	c3	[26] 21.1.4	c3	c3
5	183 (Session Progress)	[26] 21.1.5	c3	c3	[26] 21.1.5	c3	c3
102	2xx response	[26] 21.2	p22	p22	[26] 21.1	p22	p22
6	200 (OK)	[26] 21.2.1	m	m	[26] 21.2.1	i	m
7	202 (Accepted)	[28] 8.3.1	c4	c4	[28] 8.3.1	c4	c4
103	3xx response	[26] 21.3	p23	p23	[26] 21.1	p23	p23
8	300 (Multiple Choices)	[26] 21.3.1	m	m	[26] 21.3.1	i	i
9	301 (Moved Permanently)	[26] 21.3.2	m	m	[26] 21.3.2	i	i
10	302 (Moved Temporarily)	[26] 21.3.3	m	m	[26] 21.3.3	i	i
11	305 (Use Proxy)	[26] 21.3.4	m	m	[26] 21.3.4	i	i
12	380 (Alternative Service)	[26] 21.3.5	m	m	[26] 21.3.5	i	i
104	4xx response	[26] 21.4	p24	p24	[26] 21.4	p24	p24
13	400 (Bad Request)	[26] 21.4.1	m	m	[26] 21.4.1	i	i
14	401 (Unauthorized)	[26] 21.4.2	m	m	[26] 21.4.2	i	c10
15	402 (Payment Required)	[26] 21.4.3	n/a	n/a	[26] 21.4.3	n/a	n/a
16	403 (Forbidden)	[26] 21.4.4	m	m	[26] 21.4.4	i	i
17	404 (Not Found)	[26] 21.4.5	m	m	[26] 21.4.5	i	i
18	405 (Method Not Allowed)	[26] 21.4.6	m	m	[26] 21.4.6	i	i
19	406 (Not Acceptable)	[26] 21.4.7	m	m	[26] 21.4.7	i	i
20	407 (Proxy Authentication Required)	[26] 21.4.8	m	m	[26] 21.4.8	i	i
21	408 (Request Timeout)	[26] 21.4.9	m	m	[26] 21.4.9	i	i
22	410 (Gone)	[26] 21.4.10	m	m	[26] 21.4.10	i	i
22A	412 (Conditional Request Failed)	[70] 11.2.1	c20	c20	[70] 11.2.1	c19	c19
23	413 (Request Entity Too Large)	[26] 21.4.11	m	m	[26] 21.4.11	i	i
24	414 (Request-URI Too Large)	[26] 21.4.12	m	m	[26] 21.4.12	i	i
25	415 (Unsupported Media Type)	[26] 21.4.13	m	m	[26] 21.4.13	i	i
26	416 (Unsupported URI Scheme)	[26] 21.4.14	m	m	[26] 21.4.14	i	i
27	420 (Bad Extension)	[26] 21.4.15	m	m	[26] 21.4.15	i	i
28	421 (Extension Required)	[26] 21.4.16	m	m	[26] 21.4.16	i	i
28A	422 (Session Interval Too Small)	[58] 6	c8	c8	[58] 6	c8	c8
29	423 (Interval Too Brief)	[26] 21.4.17	c5	c5	[26] 21.4.17	c6	c6
29A	429 (Provide Referrer Identity)	[59] 5	c9	c9	[59] 5	c9	c9
29B	433 (Anonymity Disallowed)	[67] 4	c14	c14	[67] 4	c14	c14
30	480 (Temporarily not available)	[26] 21.4.18	m	m	[26] 21.4.18	i	i
31	481 (Call /Transaction Does Not Exist)	[26] 21.4.19	m	m	[26] 21.4.19	i	i
32	482 (Loop Detected)	[26] 21.4.20	m	m	[26] 21.4.20	i	i
33	483 (Too Many Hops)	[26] 21.4.21	m	m	[26] 21.4.21	i	i
34	484 (Address Incomplete)	[26] 21.4.22	m	m	[26] 21.4.22	i	i

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
35	485 (Ambiguous)	[26] 21.4.23	m	m	[26] 21.4.23	i	i
36	486 (Busy Here)	[26] 21.4.24	m	m	[26] 21.4.24	i	i
37	487 (Request Terminated)	[26] 21.4.25	m	m	[26] 21.4.25	i	i
38	488 (Not Acceptable Here)	[26] 21.4.26	m	m	[26] 21.4.26	i	i
39	489 (Bad Event)	[28] 7.3.2	c4	c4	[28] 7.3.2	c4	c4
40	491 (Request Pending)	[26] 21.4.27	m	m	[26] 21.4.27	i	i
41	493 (Undecipherable)	[26] 21.4.28	m	m	[26] 21.4.28	i	i
41A	494 (Security Agreement Required)	[48] 2	c7	c7	[48] 2	n/a	n/a
105	5xx response	[26] 21.5	p25	p25	[26] 21.5	p25	p25
42	500 (Internal Server Error)	[26] 21.5.1	m	m	[26] 21.5.1	i	i
43	501 (Not Implemented)	[26] 21.5.2	m	m	[26] 21.5.2	i	i
44	502 (Bad Gateway)	[26] 21.5.3	m	m	[26] 21.5.3	i	i
45	503 (Service Unavailable)	[26] 21.5.4	m	m	[26] 21.5.4	i	i
46	504 (Server Time-out)	[26] 21.5.5	m	m	[26] 21.5.5	i	i
47	505 (Version not supported)	[26] 21.5.6	m	m	[26] 21.5.6	i	i
48	513 (Message Too Large)	[26] 21.5.7	m	m	[26] 21.5.7	i	i
49	580 (Precondition Failure)	[30] 8	m	m	[30] 8	i	i
106	6xx response	[26] 21.6	p26	p26	[26] 21.6	p26	p26
50	600 (Busy Everywhere)	[26] 21.6.1	m	m	[26] 21.6.1	i	i
51	603 (Decline)	[26] 21.6.2	m	m	[26] 21.6.2	i	i
52	604 (Does Not Exist Anywhere)	[26] 21.6.3	m	m	[26] 21.6.3	i	i
53	606 (Not Acceptable)	[26] 21.6.4	m	m	[26] 21.6.4	i	i

c1: IF A.163/9 AND A.162/5 THEN m ELSE n/a - - INVITE response, stateful proxy.
c2: IF A.163/9 THEN (IF A.162/5 THEN m ELSE i) ELSE n/a - - INVITE response, stateful proxy.
c3: IF A.163/9 THEN m ELSE n/a - - INVITE response.
c4: IF A.162/27 THEN m ELSE n/a - - SIP specific event notification.
c5: IF A.163/19 OR A.163/21 THEN m ELSE n/a - - REGISTER response or SUBSCRIBE response.
c6: IF A.163/19 OR A.163/21 THEN i ELSE n/a - - REGISTER response or SUBSCRIBE response.
c7: IF A.162/47 THEN m ELSE n/a - - security mechanism agreement for the session initiation protocol.
c8: IF A.162/52 THEN m ELSE n/a - - the SIP session timer.
c9: IF A.162/53 AND A.163/17 THEN m ELSE n/a - - the SIP Referred-By mechanism and REFER response.
c10: IF A.3/2 THEN m ELSE i - - P-CSCF.
c14: IF A.162/58 THEN m ELSE n/a – rejecting anonymous requests in the session initiation protocol.
c19: IF A.162/51 THEN i ELSE n/a - - an event state publication extension to the session initiation protocol.
c20: IF A.162/51 THEN m ELSE n/a - - an event state publication extension to the session initiation protocol.
p21: A.164/2 OR A.164/3 OR A.164/4 OR A.164/5 - - 1xx response.
p22: A.164/6 OR A.164/7 - - 2xx response.
p23: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/13 - - 3xx response.
p24: A.164/14 OR A.164/15 OR A.164/16 OR A.164/17 OR A.164/18 OR A.164/19 OR A.164/20 OR A.164/21 OR A.164/22 OR A.164/22A OR A.164/23 OR A.164/24 OR A.164/25 OR A.164/26 OR A.164/27 OR A.164/28 OR A.164/28A OR A.164/29 OR A.164/29A OR A.164/29B OR A.164/30 OR A.164/31 OR A.164/32 OR A.164/33 OR A.164/34 OR A.164/35 OR A.164/36 OR A.164/436 OR A.164/38 OR A.164/39 OR A.164/40 OR A.164/41 OR A.164/41A. - - 4xx response.
p25: A.164/42 OR A.164/43 OR A.164/44 OR A.164/45 OR A.164/46 OR A.164/47 OR A.164/48 OR A.164/49 - - 5xx response.
p26: A.164/50 OR A.164/51 OR A.164/52 OR A.164/53 - - 6xx response.

A.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]	O	c1
24	Mapping of Media Streams to Resource Reservation Flows	[54]	O	c1
25	SDP Bandwidth Modifiers for RTCP Bandwidth	[56]	O	o (NOTE 1)
C1: IF A.3/1 THEN o.1 ELSE n/a - - UE role. o.1: The procedure is mandatory in case if there are access specific procedures which the UE is using. NOTE 1: For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified.				

B.2.2.6 Emergency service

When activating a PDP context for emergency to perform emergency registration, based on the conditions in subclause 5.1.6.1 of this specification, the UE shall select an APN for emergency, as described in 3GPP TS 23.060 [4]. The procedures for PDP context activation and P-CSCF discovery, as described in subclause B.2.2.1 of this specification apply accordingly.

In order to find out whether the UE is attached to the home PLMN or to the visited PLMN, the UE shall compare the MCC values derived from its IMSI with the MCC of the PLMN the UE is attached to. If the MCC of the PLMN the UE is attached to does not match with the MCC derived from the IMSI, then for the purpose of emergency calls in the IM CN subsystem the UE shall consider to be attached to a VPLMN.

NOTE: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 [4C] will be considered as a visited network.

B.3.1.1 P-Access-Network-Info header

The UE shall always include the P-Access-Network-Info header where indicated in subclause 5.1.

Annex C UICC and USIM Aspects for access to the IM CN subsystem

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

D.2.2.6 Emergency service

The details of network selection to select HPLMN or VPLMN are specified in 3GPP TS 24.234 [8C].

D.3 Application usage of SIP

D.3.1 Procedures at the UE

D.3.1.1 P-Access-Network-Info header

The UE shall always include the P-Access-Network-Info header where indicated in subclause 5.1.

Annex E IP-Connectivity Access Network specific concepts when using xDSL to access IM CN subsystem

E.2.2.6 Emergency service

If attached to network via xDSL access technology, the UE shall always consider being attached to its home operator's network for the purpose of emergency calls.

NOTE: In xDSL the UE is unable to receive any indication from the network, that would allow the UE to determine, whether it is currently attached to its home operator's network or to a different network, so the UE assumes itself always attached to the home operator's network when connected via xDSL access technology.

E.3 Application usage of SIP

E.3.1 Procedures at the UE

E.3.1.1 P-Access-Network-Info header

The UE may, but need not, include the P-Access-Network-Info header where indicated in subclause 5.1.

Annex ZA (normative): Cpc parameter definition

ZA.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.

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-Contact 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, etc.).

ZA.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.

ZA.3 Procedures at the originating UE

The cpc shall not be populated at the originating UE.

ZA.4 Procedures at the originating P-CSCF

No special requirement.

ZA.5 Procedures at the originating S-CSCF

No special requirement.

ZA.6 Procedures at the I-CSCF

No special requirement.

ZA.7 Procedures at the IBCF

No special requirement.

ZA.8 Procedures at the terminating P-CSCF

No special requirement.

ZA.9 Procedures at the AS at the originating network

The AS may populate the 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 based on their origin source.

ZA.9A Procedures at the S-CSCF at the terminating network

The S-CSCF 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.

ZA.10 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 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 UEs.			

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 UEs.			

History

Document history		
V1.1.1	July 2006	Publication
V1.8.0	July 2007	Membership Approval Procedure MV 20070921: 2007-07-24 to 2007-09-21