International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.366.4

(08/2010)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

IPCablecom

IPCablecom2 IP Multimedia Subsystem (IMS): Session Initiation Protocol (SIP) and Session Description Protocol (SDP) – Stage 3 specification

Recommendation ITU-T J.366.4

Recommendation ITU-T J.366.4

IPCablecom2 IP Multimedia Subsystem (IMS): Session Initiation Protocol (SIP) and Session Description Protocol (SDP) – Stage 3 specification

Summary

Recommendation ITU-T J.366.4 defines a call control protocol for use in the IP multimedia (IM) core network (CN) subsystem based on the session initiation protocol (SIP), and the associated session description protocol (SDP).

The Third Generation Partnership Project (3GPP) has developed the specification in a form optimized for the wireless environment. This Recommendation references the ETSI version of the 3GPP specification (ETSI TS 124 229 V6.9.0 (2005-12)) and specifies only the modifications necessary to optimize it for the cable environment.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T J.366.4	2010-08-29	9

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Recommendation ITU-T J.366.4

IPCablecom2 IP Multimedia Subsystem (IMS): Session Initiation Protocol (SIP) and Session Description Protocol (SDP) – Stage 3 specification

1 Scope

This Recommendation defines a call control protocol for use in the IP multimedia (IM) core network (CN) subsystem based on the session initiation protocol (SIP), and the associated session description protocol (SDP).

The Third Generation Partnership Project (3GPP) has developed the specification in a form optimized for the wireless environment. This Recommendation references the ETSI version of the 3GPP specification and specifies only the modifications necessary to optimize it for the cable environment.

It is an important objective of this work that interoperability between IPCablecom 2.0 and 3GPP IMS is provided. IPCablecom 2.0 is based upon 3GPP IMS, but includes additional functionality necessary to meet the requirements of cable operators. Recognizing developing converged solutions for wireless, wireline and cable, it is expected that further development of IPCablecom 2.0 will continue to monitor and contribute to IMS developments in 3GPP, with the aim of alignment of 3GPP IMS and IPCablecom 2.0.

Because this Recommendation indicates modifications from the ETSI specification [ETSI TS 124 229], the structure of the Recommendation does not follow normal ITU-T practice, so as to ease the task of the reader to correlate the two documents. The modifications are shown in clause 6.

2 References

[ETSI TS 124 229] ETSI TS 124 229 V6.9.0 (2005), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the terms defined in [ETSI TS 124 229].

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the abbreviations provided in [ETSI TS 124 229].

5 Conventions

This Recommendation uses the conventions provided in [ETSI TS 124 229].

6 Modifications to [ETSI TS 124 229]

Modifications introduced by this Recommendation are shown in revision marks. Unchanged text is replaced by ellipsis (…). Some parts of unchanged text (section numbers, etc.) may be kept to indicate the correct insertion points.

…

2 References

…

[39] RFC 4566 (July 2006): "SDP: Session Description Protocol".

[40] RFC 3315 (July 2003): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[40A] RFC 2131 (March 1997): "Dynamic host configuration protocol".

…

[74] RFC 3856 (August 2004): "A Presence Event Package for the Session Initiation Protocol (SIP)".

[75] RFC 4662 (August 2006): "A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists".

…

[78] RFC 4575 (August 2006): "A Session Initiation Protocol (SIP) Event Package for Conference State".

[79] RFC 5049 (December 2007): "Applying Signaling Compression (SigComp) to the Session Initiation Protocol (SIP)".

[80] RFC 3550 (July 2003): "RTP: A Transport Protocol for Real-Time Applications".

[81] RFC 5246 (August 2008), "The Transport Layer Security (TLS) Protocol Version 1.2".

[82] Recommendation ITU-T J.360 Appendix II: "IPCablecom quality of service architecture technical overview".

[83] RFC 5389 (October 2008): "Session Traversal Utilities for (NAT) (STUN)".

[84] RFC 5245 (April 2010) "Interactive Connectivity Establishment (ICE): A protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols".

[85] RFC 5766 (April 2010), "Traversal Using Relay NAT (TURN) Relay Extensions to Session Traversal Utilities for NAT (STUN)".

[86] RFC 5626 (October, 2009), "Managing Client Initiated Connections in the Session Initiation Protocol (SIP)".

[87] RFC 5627 (October, 2009), "Obtaining and Using Globally Routable User Agent URIs (GRUU) in the Session Initiation Protocol (SIP)".

[88] RFC 3605 (October 2003), "Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP)".

[89] RFC 3551 (July 2003), "RTP Profile for Audio and Video Conferences with Minimal Control"

[90] RFC 3890 (September 2004), "A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP)".

[91] RFC 4694 (October 2006), "Number Portability Parameters for the "tel" URI".

[92] RFC 3603 (October 2003), "Private Session Initiation Protocol (SIP) Proxy-to-Proxy Extensions for Supporting the PacketCable Distributed Call Signaling Architecture".

[93] Recommendation ITU-T J.360 Appendix V, "IPCablecom2 NAT and firewall traversal overview".

[94] Recommendation ITU-T J.365 (2006), "IPCablecom2 application manager interface".

[95] RFC 5628 (October 2009): "Registration Event Package Extension for Session Initiation Protocol (SIP) Globally Routable User Agent (GRUUs)".

[96] Recommendation ITU-T J.178 (2005), "IPCablecom CMS to CMS Signalling".

[97] RFC 3611 (November 2003), "RTP Control Protocol Extended Reports (RTCP XR)".

[98] Recommendation ITU-T J.366.7 (2010), "IPCablecom2 IP Multimedia Subsystem (IMS): Access security for IP-based services",

[99] Recommendation ITU-T J.361 (2006), "IPCablecom2 codec and media".

[100] RFC 2119 (March 1997), "Key words for use in RFCs to Indicate Requirement Levels".

[101] RFC 2616 (June 1999), "Hypertext Transfer Protocol – HTTP/1.1".

[102] RFC 2818 (May 2000), "HTTP Over TLS".

[103] RFC 3361 (August 2002), "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

[104] RFC 4122 (July 2005), "A Universally Unique IDentifier (UUID) URN Namespace".

[105] RFC 4474 (August 2006), "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)".

[106] RFC 4483 (May 2006), "A Mechanism for Content Indirection in Session Initiation Protocol (SIP) Messages".

[107] RFC 4704 (October 2006), "The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option".

[108] RFC 5226 (May 2008), "Guidelines for Writing an IANA Considerations Section in RFCs".

3 Definitions and abbreviations

• • •

3.2 Abbreviations

• • •

CDR	Charging Data Record
cic	Carrier Identification Code

• • •

CSCF	Call Session Control Function
dai	Dial-Around-Indicator

• • •

MRFP	Multimedia Resource Function Processor
npdi	Number Portability Database dip Indicator

• • •

RES	RESponse
rn	Routing Number

• • •

SQN	SeQuence Number
TLS	Transport Layer Security

• • •

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

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

Each IM CN subsystem functional entity using an interface at the Gm reference point, the Mg reference point, the Mi reference point, the Mj reference point, the 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, and the IPCablecom reference points 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 IPCablecom architecture defines a set of reference points to allow a cable IP-CAN to utilize an IMS core. Included in the IPCablecom architecture is a reference point, PKT-QOS-1 (see the IPCablecom Quality of Service Overview [82], and the IPCablecom Application Manager Interface specification [94]), that parallels the Gq reference point. Throughout this document all references to the Gq reference point shall also include reference to the PKT-QOS-1 reference point.

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

~~– The User Equipment (UE) shall provide the User Agent (UA) role, with the exceptions and additional capabilities to SIP as described in subclause 5.1, with the exceptions and additional~~

~~capabilities to SDP as described in subclause 6.1, and with the exceptions and additional capabilities to SigComp as described in subclause 8.1. The UE shall also provide the access dependent procedures described in subclause 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 thirdparty registration, the S-CSCF shall provide the UA role;~~

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

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

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

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

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

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

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

- ~~The AS, acting as a SIP proxy (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.3), shall provided the proxy role, with the exceptions and additional capabilities as described in subclause 5.7.4.~~

- ~~The AS, performing 3rd party call control (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.4), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.5, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.~~

~~NOTE 1: Subclause 5.7 and its subclauses define only the requirements on the AS that relate to SIP. Other requirements are defined in 3GPP TS 23.218 [5].~~

- ~~The AS, receiving third-party registration requests, shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.~~

- ~~The MRFC shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.8, and with the exceptions and additional capabilities to SDP as described in subclause 6.5.~~
- ~~The IMS-ALG shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.9, and with the exceptions and additional capabilities to SDP as described in subclause 6.5.~~

~~In addition to the roles specified above, the P-CSCF, the I-CSCF, the S-CSCF, the BGCF 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.~~

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~~v6~~ addresses. For systems providing access to IMS using a fixed broadband interconnection, any IM CN subsystem entity can be allocated IPv4 only, IPv6 only or both IPv4 and IPv6 addresses. Otherwise, systems shall support IP addresses as ~~in accordance with the constraints~~ specified in 3GPP TS 23.221 [6] subclause 5.1.

3) The subscriber is allocated a private user identity by the home network operator, and this is contained within the ISIM application, if present. Where no ISIM application is present but USIM is present, the private user identity is derived (see subclause 5.1.1.1A). The mechanism for deriving the private user identity when there is no ISIM or USIM is out-of-scope. This private user identity is available to the SIP application within the UE.

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

4) The subscriber is allocated one or more public user identities by the home network operator. 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 these is SIP URI and it is contained 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 has 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.

4.2A Transport mechanisms

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

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

When a security association is used to access IMS, t~~T~~he UE and the P-CSCF shall send and receive request and responses other th~~e~~an initial REGISTER requests on the protected ports as described in ~~3GPP TS 33.203~~ITU-T J.366.7 [~~19~~98].

• • •

5 Application usage of SIP

5.1 Procedures at the UE

5.1.1 Registration and authentication

5.1.1.1 General

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

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

If signalling security is disabled, the UE shall not establish a security association toward the P-CSCF. The UE shall consider signalling security to be disabled if:

– signalling security is disabled in the UE via configuration mechanisms outside the scope of this specification and the P-CSCF is not configured to require signalling security; or

– signalling security is disabled in the P-CSCF.

NOTE – The UE determines that signalling security is disabled or required in the P-CSCF based on an indication received from the P-CSCF during initial registration.

5.1.1.1A Parameters contained in the ISIM

The ISIM application shall always be used for IMS authentication, if it is present, as described in ~~3GPP TS 33.203~~ITU-T J.366.7 [~~19~~98].

• • •

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 Instance ID

Each UE shall contain a unique Instance ID parameter, as specified in RFC 5626 [86].

This instance ID shall be used by the UE for all registrations and dialogs in which it participates, and shall remain constant for the duration of each registration and dialog in which it is used.

The instance ID should remain constant for the lifetime of the UE. For hardware devices that contain only one UE, the instance ID may be based on a MAC address of the device.

NOTE – The instance ID serves as an identifier that permits a particular UE to be recognized over time. Other identifiers, such as an IP address, often can only be obtained for a limited duration and so do not have this property. Identifiers such as the Public User Identity and the Private User Identity may need to be shared with other UEs and so also may not have the desired property. An instance ID must remain constant for at least the lifetime of a session or registration in which it is provided. A UE may change its instance ID during its lifetime, but doing so will be perceived by others as if the UE had been replaced by another.

5.1.1.2 Initial registration

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

The UE shall send only the initial REGISTER requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial REGISTER request to the SIP default port values as specified in RFC 3261 [26].

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

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

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

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

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

d) a Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the UE supports GRUU, it shall include a +sip.instance parameter containing the instance ID specified in section 5.1.1.1B. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter. The UE shall also include a reg-id as described in RFC 5626 [86];

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 an IPsec security association or a TLS session, the UE shall also include the protected server port value in the sent-by field. If the REGISTER request is not protected by a security association, the UE shall also include the rport parameter as defined in RFC 3581 [56A];

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 – For IPsec, t~~T~~he 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~~ ITU-T J.366.7 [~~19~~98].

NOTE 2a – For TLS, see ITU-T J.366.7 [98] for details on the selection of the protected port value.

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) if signalling security is not disabled, 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. For IPsec, t~~T~~he UE shall support the setup of two pairs of security associations as defined in ~~3GPP TS 33.203~~ITU-T J.366.7 [~~19~~98]. The syntax of the parameters needed for the IPsec security association setup is specified in Annex H of ~~3GPP TS 33.203~~ITU-T J.366.7 [~~19~~98]. The UE shall support the "ipsec-3gpp" and "tls" security mechanisms, 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]. The UE shall support TLS ciphersuites as described in ITU-T J.366.7 [98];

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

j) if a security association exists and if the access network type is available to the UE, 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) if it supports the P-Associated-URI header, 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) if it supports the P-Associated-URI header, 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 and the UE supports the P-Associated-URI header;

e) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions; and

f) If IPsec security associations are established, 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~~.~~,

g) locate the Contact header within the response that matches the one included in the REGISTER request. If this contains a 'gruu' parameter, and the UE supports GRUU, then store the value of the 'gruu' parameter in association with the public user identity that was registered.

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

On receiving a 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.

Procedures described in RFC 5626 [86] for forming requests and handling responses shall be followed.

When a 420 (Bad Extension) response to the REGISTER request is received that includes an Unsupported header containing the value "sec-agree", the UE shall consider signalling security as disabled in the P-CSCF and may re-attempt initial registration by sending another REGISTER request according to the above procedures.

When a 494 (Security Agreement Required) response to the REGISTER request is received, the UE shall consider signalling security as required in the P-CSCF and should re-attempt initial registration by sending another REGISTER request according to the above procedures.

NOTE 4 – It is an implementation option for the UE to remember the P-CSCF signalling security configuration (i.e., disabled or required) so that future registration attempts are more efficient.

5.1.1.3 Initial subscription to the registration-state event package

Support for the registration-state event package is optional at the UE. A UE that does not support the registration-state event package does not need to support the following procedures.

Upon receipt of a 2xx response to the initial registration, and if the registration-state event package is supported, 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 a security association exists and if the access network type is available to the UE, 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 if signalling security is not disabled, 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

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

In particular, a UE shall follow the requirements in RFC 5626 [86] in re-registering to create a flow in the case of a flow failure.

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 or TLS session (if present), see ~~3GPP TS 33.203~~ITU-T J.366.7 [~~19~~98], established as a result of an earlier registration, if IK is available (if using IPsec).

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~~. If signalling security is not disabled, the UE shall also include the protected server port value bound to the security association or TLS session. The UE shall also include a +sip.instance parameter containing the instance ID specified in section 5.1.1.1B, and a reg-id as described in RFC 5626 [86];

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field~~ and~~. If signalling security is not disabled, the UE shall also include the protected server port value bound to the security association~~;~~ or TLS session. If the REGISTER request is not protected by a security association, the UE shall also include the rport parameter as defined in RFC 3581 [56A];

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 – For IPsec, t~~T~~he 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~~ITU-T J.366.7 [~~19~~98].

NOTE 2a – For TLS, see ITU-T J.366.7 [98] for details on the selection of the protected port value.

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) if signalling security is not disabled, a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer or TLS algorithms it supports and the new parameter values needed for the setup of two new pairs of IPsec security associations or a TLS session. For further details see ~~3GPP TS 33.203~~ITU-T J.366.7 [~~19~~98] and RFC 3329 [48];

i) if signalling security is not disabled, 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) if a security association exists and if the access network type is available to the UE, 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 new expiration time of the registration for this public user identity found in the To header value;

b) if it supports the P-Associated-URI header, store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;

c) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs and standalone transactions; ~~and~~

d) if IPsec security associations are established, 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~~.~~;

e) locate the Contact header within the response that matches the one included in the REGISTER request. If this contains a 'gruu' parameter, and the UE supports GRUU, then store the value of the 'gruu' parameter in association with the public user identity that was registered, replacing any value previously associated.

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

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

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

On receiving a 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 associated with that flow 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~~ shall follow the procedures in clause 4.1 to form a new flow to replace the failed one. When registering to create a new flow to replace the failed one, procedures in subclause 5.1.1.2 apply~~.~~:

~~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 4 – These actions may also be triggered as a result of the failure of a STUN keep-alive. It is an implementation option whether these actions are also triggered by other means than expiration of timer F, e.g., based on ICMP messages.

If failed registration attempts occur in the process of creating a new flow, the procedures defined in RFC 5626 [86] shall apply.

~~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 Authentication

5.1.1.5.1 General

Authentication is achieved via the registration and re-registration procedures. When the network requires authentication or re-authentication of the UE, the UE will receive a 401 (Unauthorized) response to the REGISTER request.

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

1) if the algorithm parameter is AKAv1-MD5, extract the RAND and AUTN parameters;

2) if the algorithm parameter is AKAv1-MD5, check the validity of a received authentication challenge, as described in ~~3GPP TS 33.203~~ITU-T J.366.7[~~19~~98] 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) if signalling security is not disabled, check the existence of the Security-Server header as described in RFC 3329 [48]. If the header is not present or if for IPsec it does not contain the parameters required for the setup of the set of security associations (see annex H of ~~3GPP TS 33.203~~ITU-T J.366.7[~~19~~98]), 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 and signalling security is not disabled, the UE shall:

1) if the algorithm parameter is AKAv1-MD5: calculate the RES parameter and derive the keys CK and IK from RAND as described in ~~3GPP TS 33.203~~ITU-T J.366.7[~~19~~98];

2) for IPsec, 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

2a) for TLS, the UE sets up the TLS session as described in ITU-T J.366.7 [98];

3) send another REGISTER request using the temporary set of IPsec security associations or TLS session to protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the private user identity and if the algorithm is AKAv1-MD5, the authentication challenge response calculated by the UE using RES and other parameters, as described in

RFC 3310 [49]. If the algorithm is MD5, the authentication challenge response calculated by the UE using the nonce and other parameters, as described in ITU-T J.366.7 [98]. 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.

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

- if the algorithm parameter is AKAv1-MD5, calculate the RES parameter and derive the CK and IK from RAND as described in ITU-T J.366.7 [98];
- if the algorithm is MD5 or SHA1, calculate the response as described in ITU-T J.366.7 [98];
- send another REGISTER request. 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 not include RFC 3329 headers. The UE shall set the Call_ID of the REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

~~On~~If signalling security is not disabled, then upon receiving the 200 (OK) response for the integrity protected REGISTER request, the UE shall:

- change the temporary set of IPsec security associations to a newly established set of IPsec 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 IPsec security associations or TLS session for further messages sent towards the P-CSCF as appropriate.

NOTE 1 – In the~~is~~ case of IPsec, 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.

If IPsec security associations are established, then ~~W~~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.

If IPsec security associations are established, then w~~W~~henever 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.

If a TLS session is established and a 403 (Forbidden) response is received, the UE shall consider the registration to have failed. The UE should send an initial REGISTER according to the procedure specified in subclause 5.1.1.2 using the existing TLS session.

If signalling security is disabled and a 403 (Forbidden) response is received, the UE shall consider the registration to have failed. The UE should send an initial REGISTER message according to the procedure specified in subclause 5.1.1.2.

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

5.1.1.5.2 Network-initiated re-authentication

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

– the state attribute in any of the <registration> elements is set to "active";

– the value of the <uri> sub-element inside the <contact> sub-element is set to the Contact address that the UE registered; and

– the event attribute of that <contact> sub-element(s) is set to "shortened";

the UE shall:

1) use the expiry attribute within the <contact> sub-element that the UE registered to adjust the expiration time for that public user identity; and

2) start the re-authentication procedures at the appropriate time (as a result of the S-CSCF procedure described in subclause 5.4.1.6) by initiating a reregistration as described in subclause 5.1.1.4, if required.

NOTE – When authenticating a given private user identity, the S-CSCF will only shorten the expiry time within the <contact> sub-element that the UE registered using its private user identity. The <contact> elements for the same public user ~~identitity~~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.

5.1.1.5.3 Abnormal cases

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

– in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no authentication challenge response and no AUTS parameter;

– in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the AUTS parameter and not an authentication challenge response (see 3GPP TS 33.102 [18]).

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

– send the REGISTER request using an existing set of IPsec security associations or TLS session, if available (see ~~3GPP TS 33.203~~ITU-T J.366.7 [~~19~~98]);

– if signalling security is not disabled, populate a new Security-Client header within the REGISTER request, set to specify the security mechanism it supports, the ~~IPsec layer~~ algorithms it supports and the parameters needed for the new security association setup; and

– if negotiating IPsec, not create a temporary set of security associations.

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

5.1.1.5A Change of 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 ~~subselause~~subclause 5.1.1.4;

3) construct a new IPv6 address according to the procedures specified in RFC 3041 [25A];

4) register the public user identities that were deregistered in step 2 above, as follows:

   a) by performing an initial registration as described in ~~subselause~~subclause 5.1.1.2; and

   b) by performing a subscription to the reg event package as described in ~~subselause~~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

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 or TLS session, see ~~3GPP TS 33.203~~ITU-T J.366.7 [~~19~~98], 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.

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~~. If a security association exists, the UE shall also include the protected server port value bound to the security association or TLS session;

e) a Via header set to include the IP address or FQDN of the UE in the sent-by field~~ and~~. If a security association exists, the UE shall also include the protected server port value bound to the security association or TLS session. If signalling security is disabled, the UE shall also include the rport parameter as defined in RFC 3581 [56A];

   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 or TLS session.

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 a security association exists and if the access network type is available to the UE, 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 or TLS session (if present) and related keys it may have towards the IM CN subsystem.

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

NOTE – When the UE has received the 200 (OK) response for the REGISTER request of the only public user identity currently registered with its associated set of implicitly registered public user identities (i.e., no other is registered) and signalling security is not disabled, the UE removes the security association or TLS session established between the P-CSCF and the UE. Therefore further SIP signalling (e.g., the NOTIFY request containing the deregistration event) will not reach the UE.

5.1.1.7 Network-initiated deregistration

If the UE supports the registration-state event package and u~~U~~pon 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. 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 or TLS session (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 or TLS session 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 or TLS session 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 or TLS session established between the P-CSCF and the UE, further SIP signalling (e.g., the NOTIFY containing the deregistration event) will not reach the UE.

5.1.2 Subscription and notification

NOTE – These procedures apply to the UE only if it supports the registration-state event package.

5.1.2.1 Notification about multiple registered public user identities

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

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

- if a state attribute "active", i.e., registered is received for one or more public user identities, the UE shall store the indicated public user identities as registered;
- if a state attribute "active" is received, and the UE supports GRUU, then for each public user identity indicated in the notification that contains a <gruu> element (as defined in RFC 5628 [95]) then the UE shall store the value of the 'gruu' element in association with the public user identity, replacing any value previously associated;
- if a state attribute "init" or "terminated", i.e., deregistered is received for one or more public user identities, the UE shall store the indicated public user identities as deregistered, and shall remove any associated gruu.

  NOTE – There may be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity. Usually these automatically or implicitly registered public user identities belong to the same service profile of the user and they might not be available within the UE. The implicitly registered public user identities may also belong to different service profiles. The here-described procedures provide a different mechanism (to the 200 (OK) response to the REGISTER request) to inform the UE about these automatically registered public user identities.

5.1.2.2 General SUBSCRIBE requirements

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

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

5.1.2A.1 Mobile-originating case

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

If a security association or TLS session exists, ~~W~~when the UE sends any request, the UE shall:

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

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

If no security association exists, when the UE sends any request, the UE shall include the rport parameter in the Via header as defined in RFC 3581 [56A].

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

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

– a public user identity which has been registered by the user;

– a public user identity returned in a registration-state event package (if supported by the UE) of a NOTIFY request as a result of an implicit registration that was not subsequently deregistered or has expired; ~~or~~

– any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration~~.~~; or

– an unregistered public user identity, if the UE determines that the request is a SUBSCRIBE request for the ua-profile event package. The mechanism to determine the public user identity to include in the request is outside the scope of this specification.

NOTE 1 – The temporary public user identity specified in subclause 5.1.1.1 is not a public user identity suitable for use in the P-Preferred-Identity header.

NOTE 2 – Procedures in the network require international public telecommunication numbers when telephone numbers are used in P-Preferred-Identity header.

NOTE 3 – 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 3a – Local policy may allow the UE to send a SUBSCRIBE request to the ua-profile event package prior to registration.

NOTE 3b – If the UE does not insert a P-Preferred-Identity header and no security association exists, the From header is used as a hint for creation of an asserted identity within the IM CN subsystem. In this case, the UE shall include in the From header a public user identity selected according to the above procedures for P-Preferred-Identity.

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". If no security association or TLS session exists, the UE shall insert a P-Preferred-Identity header.

NOTE 4 – 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].

NOTE 4a – To obtain full functionality, the UE needs to ensure that the address it includes in a Contact header identifies the UE in a way that allows resulting communications to reach the UE. Some features may not work correctly unless the contact address used in a dialog may also be used outside that dialog to reach the same UE. The UE's IP address often cannot be used this way because of NATs and the need to reuse the security association between the UE and the P-CSCF. The use of a GRUU as a contact address permits out-of-dialog requests to reach the UE and still use the security association the UE has established. The following step causes a GRUU to be used when possible.

If the request is to include a Contact header, then the UE shall perform the following:

1) Determine the public user identity to be used for this request:

   a) if a P-Preferred-Identity was included, then use that as the public user identity for this request;

   b) if no P-Preferred-Identity was included, but a security association exists, then use the default public user identity for the security association as the public user identity for this request;

   c) if no P-Preferred-Identity was included, and no security association exists, then use the URI in the From header as the public user identity for this request;

   d) otherwise consider the public user identity to be used for this request to be unknown.

2) If the public user identity for this request is known, and the UE supports GRUU, and a gruu value has been saved associated with the public user identity to be used for this request the UE should insert the GRUU in the Contact header.

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

If a security association or TLS session exists and if the access network type is available, the~~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 5 – 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 (if signalling security is not disabled)), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration if the user is registered.

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.

5.1.2A.2 Mobile-terminating case

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

~~When the UE sends any response, the UE shall:~~

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

If a security association or TLS session exists, t~~T~~he UE shall discard any SIP request that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

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

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

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

If the UE supports GRUU, then the gruu associated with the local public user identity for this request is used in the Contact header (if present) of the response. The UE shall determine the local public user identity for this request, as follows:

1) if this is a request within a dialog, use the local public user identity of this dialog;

2) if this is not a request within a dialog, and it contains a P-Called-Party-Identity header, then the value of the P-Called-Party-Identity header is the local public user identity;

3) otherwise the local public user identity for this request may be chosen from any public user identity the UE supports.

If the request establishes a dialog, then the UE shall save the determined local public user identity of this request as an attribute of the dialog.

If the response is to include a Contact header, then the UE shall adjust the value to be included in the Contact header as follows:

1) Determine the gruu to be used for this response:

   a) If the UE supports GRUU, and a gruu value has been saved associated with the local public user identity, then the UE should use the saved gruu value as the gruu for this response;

   b) otherwise there is no gruu for this response.

2) If there is a gruu for this response, then:

   a) insert it in the Contact header;

   b) insert a Supported header in the response containing the value 'gruu'.

3) If there is no gruu for this response, and a security association or TLS session exists, then include the protected server port in the address present in the Contact header.

If a security association or TLS session exists and if the access network type is available, the~~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).

5.1.3 Call initiation – mobile originating case

5.1.3.1 Initial INVITE request

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

The precondition mechanism should be supported by the originating UE.

The UE may initiate a session without the precondition mechanism if the originating UE does not require local resource reservation.

NOTE 1 – The originating UE can decide if local resource reservation is required based on e.g., application requirements, current access network capabilities, local configuration, etc.

In order to allow the peer entity to reserve its required resources prior to session establishment, an originating UE supporting the precondition mechanism should make use of the precondition mechanism, even if it does not require local resource reservation.

Upon generating an initial INVITE request using the precondition mechanism, if the UE is configured to require the support of preconditions, then the UE shall:

- indicate the support for reliable provisional responses and specify it using the Require header mechanism; and
- indicate the support for the preconditions mechanism and specify it using the Require header mechanism.

Upon generating an initial INVITE request using the precondition mechanism, if the UE is configured to negotiate the use of preconditions with the remote UE, then the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism; and
- indicate the support for the preconditions mechanism and specify it using the Supported header mechanism.

~~Upon generating an initial INVITE request using the precondition mechanism, the UE should not indicate the requirement for the precondition mechanism by using the Require header mechanism.~~

NOTE 2 – If an UE chooses to require the precondition mechanism, i.e., if it indicates the "precondition" option tag within the Require header, the interworking with a remote UE, that does not support the precondition mechanism, is not described in this specification.

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

NOTE 3 – Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26]. The UE can accept or reject any of the forked responses, for example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs.

Upon successful reservation of local resources the UE shall confirm the successful resource reservation (see subclause 6.1.2) within the next SIP request.

NOTE 4 – In case of the precondition mechanism being used on both sides, this confirmation will be sent in either a PRACK request or an UPDATE request. In case of the precondition mechanism not being supported on one or both sides, alternatively a reINVITE request can be used for this confirmation (after the initial INVITE transaction has completed), in case the terminating UE does not support the PRACK request (as described in RFC 3262 [27]) and does not support the UPDATE request (as described in RFC 3311 [29]).

When a final answer is received for one of the early dialogues, the UE proceeds with~~to set up~~ the SIP session. The UE shall not progress any remaining early dialogues to established dialogs. Therefore, upon the reception of a subsequent final 200 (OK) response for an INVITE request (e.g., due to forking), the UE shall:

1) acknowledge the response with an ACK request; and
2) send a BYE request to this dialog in order to terminate it.

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

NOTE 5 – An example of where a new request would not be sent is where knowledge exists within the UE, or interaction occurs with the user, such that it is known that the resulting SDP would describe a session that did not meet the user requirements.

Upon receiving a 421 (Extension Required) response to an initial INVITE request in which the precondition mechanism was not used, including the "precondition" option tag in the Require header, the originating UE shall send a new INVITE request using the precondition mechanism, if the originating UE supports the precondition mechanism.

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

The UE should support the client requirements for ICE as defined by RFC 5245 [84]. This includes:

1) Gathering of addresses for RTP and RTCP prior to sending the INVITE as described in section 7.1 of RFC 5245 [84]. The client shall act as a STUN client as described in RFC 5389 [83] in order to gather STUN addresses. It shall also act as a TURN client as described in RFC 5766 [85] in order to gather TURN addresses.

2) Encoding the candidate addresses in the SDP that is included with the INVITE as described in section 7.3 of RFC 5245 [84].

3) Acting as a STUN server to receive binding requests from the remote client when it does connectivity checks. The UE shall support the requirements defined in sections 7.6 and 7.8 of RFC 5245 [84] as well as the requirements for STUN servers defined in RFC 5389 [83].

4) Once the UE receives the answer to its offer with candidate addresses, it shall send binding requests in order to do connectivity checks as defined in section 7.7 of RFC 5245 [84]. This requires that it act as a STUN client as defined in RFC 5389 [83].

5) It shall then determine and possibly select a better active address based on the requirements in section 7.9 of RFC 5245 [84].

6) It shall follow the requirements in section 7.11 of RFC 5245 [84] for any subsequent offer/answer exchanges.

7) It shall follow section 7.13 of RFC 5245 [84] when sending media.

Section 7.2 of RFC 5245 [84] does not include any normative requirements for prioritizing address candidates and selecting the active transport address. The requirements for the UE are specified as follows:

1) If a TURN server is available, the TURN address should be used as the initial active transport address (i.e., as advertised in the m/c lines of the SDP).

2) If a TURN server is not available, an address obtained via STUN should be used as the initial active transport address.

3) The priority of candidate addresses from least to highest should be: TURN address, STUN address, local address.

4) If the UE has a dual IPv4/IPv6 stack, IPv6 addresses MAY be placed at a higher priority than IPv4 addresses based on the operator's policy.

The UE may include a "cic" parameter in a tel URI in the Request-URI of an initial INVITE request, if the UE wants to identify a user-dialed carrier (as described in RFC 4694 [91]).

5.1.4 Call initiation – mobile terminating case

5.1.4.1 Initial INVITE request

The precondition mechanism should be supported by the terminating UE.

The handling of incoming initial INVITE requests at the terminating UE is mainly dependent on the following conditions:

– the specific service requirements for "integration of resource management and SIP" extension (hereafter in this subclause known as the precondition mechanism and defined in RFC 3312 [30] as updated by RFC 4032 [64], and with the request for such a mechanism known as a precondition); and

– the UEs configuration for the case when the specific service does not require the precondition mechanism.

Editor's Note – The detailed criteria when to use the non-precondition procedures / resource reservation should be either derived from stage 2 or should be included as a reference to 3GPP TS 23.228.

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1 – The terminating UE can decide if local resource reservation is required based on e.g., application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and:

a) the received INVITE request includes the "precondition" option-tag in the Supported or Require header, the terminating UE shall make use of the precondition mechanism and indicate it by setting the "precondition" and "100rel" option-tags in the Require header in the response to the received INVITE; or

b) the received INVITE request does not include the "precondition" option-tag in the Supported or Require header the terminating UE shall not make use of the precondition mechanism.

If local resource reservation is not required by the terminating UE and the terminating UE supports the precondition mechanism and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header and

– the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism; or

– the required local resources at the originating UE and the terminating UE are available, the terminating UE may use the precondition mechanism; or

aa) the received INVITE request includes the "precondition" option-tag in the Require header, the terminating UE shall make use of the precondition mechanism;

b) the received INVITE request does not include the "precondition" option-tag in the Supported or Require header, the terminating UE shall not make use of the precondition mechanism.

NOTE 2 – Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26].
Editor's Note: The above note needs further investigation.

NOTE 3 – If the terminating UE does not support the precondition mechanism it will apply regular SIP session initiation procedures.

If the INVITE indicated support for reliable provisionable responses, but did not require their use, t~~T~~he terminating UE shall send provisional responses reliably only if the provisional response carries SDP or other application related data that requires its reliable transport.

The UE should support client requirements for ICE as defined by RFC 5245 [84]. This includes:

1) It shall gather addresses for RTP and RTCP prior to sending the answer as described in RFC 5245 [84]. The UE shall act as a STUN client as described in RFC 5389 [83] in order to gather STUN addresses. It shall also act as a TURN client as described in RFC 5766 [85] in order to gather TURN addresses.

2) Encoding the candidate addresses in the SDP answer as described in RFC 5245 [84].

3) Allowing the remote UE to do connectivity checks by accepting STUN binding requests as described in RFC 5245 [84]. This requires that the UE act as a STUN server as defined in RFC 5389 [83].

4) It shall then determine and possibly select a better active address based on the requirements in RFC 5245 [84].

5) It shall follow the requirements in RFC 5245 [84] for any subsequent offer/answer exchanges.

Regardless of whether the UE supports the above procedures, the UE shall, upon receipt of an offer with candidate addresses, perform connectivity checks on the candidate addresses as described in RFC 5245 [84]. In order to do that it shall act as a STUN client as defined in RFC 5389 [83]. Further, the UE shall also follow the procedures in RFC 5245 [84] when sending media.

RFC 5245 [84] does not include any normative requirements for prioritizing address candidates and selecting the active transport address. The requirements for the UE are specified as follows:

1) If a TURN server is available, the TURN address should be used as the initial active transport address (i.e., as advertised in the m/c lines of the SDP).

2) If a TURN server is not available, an address obtained via STUN should be used as the initial active transport address.

3) The priority of candidate addresses from least to highest should be: TURN address, STUN address, local address.

4) If the UE has a dual IPv4/IPv6 stack, IPv6 addresses MAY be placed at a higher priority than IPv4 addresses based on the operator's policy.

5.1.5 Call release

Void.

5.1.6 Emergency service

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

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a XML body that includes an <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.

5.1.7 Void

5.1.8 Maintaining flows and detecting flow failures

STUN binding requests are used by the UE as a keep-alive mechanism to maintain NAT bindings for signalling flows (for dialogs outside a registration as well as within a registration) as well as to determine whether a flow (as described in RFC 5626 [86]) is still valid (e.g., a NAT reboot could cause the transport parameters to change). As such, the UE acts as a STUN client and shall follow the requirements defined by RFC 5389 [83].

NAT bindings also need to be kept alive for media. In order to do that, the UE shall support the requirements described in RFC 5245 [84]. In the case where keep-alives are required and the other end does not support ICE (such that STUN cannot be used for a keep-alive), the UE shall send an empty (no payload) RTP packet with a payload type of 20 as a keep-alive as long as the other end has not negotiated the use of this value. If this value has already been negotiated, then some other unused static payload type from Table 5 of RFC 3551 [89] shall be used. When sending an empty RTP packet, the UE shall continue using the sequence number (SSRC) and timestamp as the negotiated RTP steam.

5.2 Procedures at the P-CSCF

5.2.1 General

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

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

When the P-CSCF sends any request or response to the UE, before sending the message the P-CSCF shall:

- remove the P-Charging-Function-Addresses and P-Charging-Vector headers, if present.

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

- remove the P-Charging-Function-Addresses and P-Charging-Vector headers, if present. Also, the P-CSCF shall ignore any data received in the P-Charging-Function-Addresses and P-Charging-Vector headers; and
- may insert previously saved values into the P-Charging-Function-Addresses and P-Charging-Vector headers before forwarding the message.

NOTE 2 – When the P-CSCF is located in the visited network, then it will not receive the P-Charging-Function-Addresses header from the S-CSCF or I-CSCF. Instead, the P-CSCF discovers charging function addresses by other means not specified in this document.

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

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

The P-CSCF can be configured to have signalling security required, disabled or optional:

- If signalling security is required, the P-CSCF shall require the establishment of a security association or TLS session toward all UE, in order to access IMS subsequent to registration.
- If signalling security is disabled, the P-CSCF shall not establish a security association or TLS session toward any UE.
- If signalling security is optional, the P-CSCF determines whether to establish a security association or TLS session toward a UE on a per registration basis. In this case, the P-CSCF shall establish a security association toward a UE if the initial REGISTER request contains a Security-Client header field, otherwise the P-CSCF shall not establish a security association toward the UE.

NOTE 3a – The mechanism to configure the P-CSCF to have signalling security mandatory, disabled or optional is outside the scope of this specification.

NOTE 4 – If a security association or TLS session was established, t~~T~~he P-CSCF will integrity protect all SIP messages sent to the UE outside of the registration and authentication procedures. The P-CSCF will discard any SIP message that is not ~~integirity~~integrity protected and is received outside of the registration and authentication procedures. The integrity protection and checking requirements on the P-CSCF within the registration and authentication procedures are defined in subclause 5.2.2.

5.2.2 Registration

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

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

1) insert a Path header in the request including an entry containing:
   - the SIP URI identifying the P-CSCF;
   - an indication that requests routed in this direction of the path (i.e., from the S-CSCF to

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

– a flow identifier token as described in RFC 5626 [86].

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 or mutually authenticated TLS session 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";

4A) check if the REGISTER request contains a P-Access-Network-Info header field:

a) if the header is present and the REGISTER request was received without integrity protection, then the P-CSCF shall remove it;

b) if the header is not present or was removed by the P-CSCF, and the access network type being used by the UE is known, then the P-CSCF shall insert a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4);

4B) in case the REGISTER request was received without integrity protection, then check if the Via header contains the rport parameter with no value. If present, then the P-CSCF shall set the value of the parameter to the source port of the request as defined in RFC 3581 [56A];

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 and signalling security is not disabled, then remove and store it. If the header is present and signalling security is disabled, then the P-CSCF shall return a 420 (Bad Extension) response and include an Unsupported header containing the value "sec-agree". If the header is ~~not present~~absent and signalling security is required, 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 or the register was protected with a TLS session, 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) for IPsec, 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; and

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

If the selected I-CSCF:

– 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 I-CSCF and forward the original REGISTER request.

NOTE 1 – The list of the I-CSCFs may 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 I-CSCF, 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].

If signalling security is not disabled, then w~~W~~hen the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request that contained a Security-Client header, the P-CSCF shall:

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

2) for IPsec, 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~~ITU-T J.366.7[~~19~~98]. The P-CSCF shall support the "ipsec-3gpp" and "tls" security mechanisms, 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. The P-CSCF shall support TLS ciphersuites as described in ITU-T J.366.7 [98];

4) for IPsec, 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~~ITU-T J.366.7 [~~19~~98] 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 or TLS session with which the associated REGISTER request was protected, or unprotected in case the REGISTER request was received unprotected.

NOTE 2 – 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 for IPsec or a TLS session with the UE during the same registration procedure. For further details see ~~3GPP TS 33.203~~ITU-T J.366.7 [~~19~~98].

If signalling security is disabled, then when the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall send the 401 (Unauthorized) response to the UE unprotected.

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

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

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

3) store the public user identities found in the P-Associated-URI header value and associate them to the public user identity under ~~regististation~~registration;

4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

   NOTE 3 – There may be more than one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

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

5a) if no security association or TLS session exists, the P-CSCF shall send the 200 (OK) response to the UE unprotected as defined in Section 4 of RFC 3581 [56A], skip the execution of step 6 onwards and ignore the remaining procedures of this subclause;

6) if an existing set of IPsec 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 IPsec 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.

For IPsec, w~~W~~hen 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 4 – 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 5 – 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 receiving a SIP message (including REGISTER requests) from the UE over an existing TLS session, the P-CSCF shall send requests and further messages towards the UE over the TLS session.

Responses towards a UE with an existing TLS session shall be via TCP.

When the SIP level lifetime of an old set of IPsec security associations is about to expire, i.e., their SIP level lifetime is ~~shorther~~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 ~~estabslihed~~established set of security associations for further messages towards the UE as appropriate (see Note 3).

When sending the 200 (OK) response for a REGISTER request that concludes a re-authentication, the P-CSCF shall:

1) for IPsec, keep the set of security associations that was used for the REGISTER request that initiated the re-authentication;

2) for IPsec, keep the newly established set of security associations created during this authentication;

3) for IPsec, 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 or TLS session that was used to protect the REGISTER request that initiated the re-authentication.

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

1) if signalling security is not disabled, keep the newly established set of security associations or TLS session created during this authentication;

2) delete, if existing, any other set of security associations towards this UE immediately; and

3) if signalling security is not disabled, use the kept newly established set of security associations or TLS session for further messages sent towards the UE.

NOTE 6 – 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~~ IPsec 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

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
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

• • •

5.2.5.1 User-initiated deregistration

When the P-CSCF receives a 200 (OK) response to a REGISTER request (sent according to subclause 5.2.2) sent by this UE, 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 or TLS session (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 the security association or TLS session (if present) 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~~the~~ security associations towards the UE.

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

NOTE 2 – When the P-CSCF receives the NOTIFY request with Subscription-State header containing the value of "terminated", the P-CSCF considers the subscription to the reg event package terminated (i.e., as if the P-CSCF had sent a SUBSCRIBE request to the S-CSCF with an Expires header containing a value of zero).

• • •

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 that is protected by a security association or TLS session, and the request contains a P-Preferred-Identity header that matches one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction that is protected by a security association or TLS session, 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 1 – The contents of the From header do not form any part of this decision process.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction that is not protected by a security association, the P-CSCF shall:

1) if signalling security is required in the P-CSCF, the P-CSCF shall do either of the following:

   a) reject the request with a 400 (Bad Request) response or silently discard the request; or

   b) if it is a SUBSCRIBE request for the ua-profile event package and local policy allows such requests prior to registration, continue with the execution of step 2;

2) if the request does not contain a P-Preferred-Identity header, and the From header contains an anonymous value, reject the request with a 400 (Bad Request) response;

3) identify the initiator of the request by the public user identity contained in the P-Preferred-Identity header if present, or the From header otherwise, and continue with the procedures

below.

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-~~CSCFshall~~ 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;

1A) in case the request was received without signalling security, then check if the Via header contains the rport parameter with no value. If present, then the P-CSCF shall set the value of the parameter to the source port of the request as defined in RFC 3581 [56A];

2) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF in accordance with the procedures of RFC3261 [26], and either:

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

   b) the P-CSCF IP address;

3) 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;

4) if the received request was protected by a security association or TLS session, remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

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

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

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26] the P-CSCF shall ensure that all signalling during the lifetime of the dialogue is sent over the same flow (source IP and Port/destination IP and Port) as the dialogue initiating request.

NOTE 1a – The suggested way to ensure all signalling is sent over the same flow is to form a flow identifier token in the same way that a P-CSCF would form this for the Path header and insert this flow identifier token in the user portion of the URI used in the Record-Route header field value.

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

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

2) store the list of Record-Route headers from the received response;

3) store the dialog ID and associate it with the private user identity and public user identity involved in the session;

4) if a security association or TLS session exists, rewrite the port number of its own Record

Route entry to its own protected server port number negotiated with the calling UE~~, and append the comp parameter in accordance with the procedures of RFC 3486 [55]~~; and

NOTE 2 – For IPsec, t~~T~~he 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~~ITU-T J.366.7 [~~19~~98].

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 3581 [56A] and 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 relate~~s~~ 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;

2a) in case the request was received without signalling security, then check if the Via header contains the rport parameter with no value. If present, then the P-CSCF shall set the value of the parameter to the source port of the request as defined in RFC 3581 [56A];

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~~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, 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 or TLS session 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 append the comp parameter in accordance with the procedures of RFC 3486 [55]~~; 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 3581 [56A] and 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 received request was protected by a security association or TLS session, remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request; and

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

4) in case the request was received without signalling security, then check if the Via header contains the rport parameter with no value. If present, then the P-CSCF shall set the value of the parameter to the source port of the request as defined in RFC 3581 [56A];

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26] the P-CSCF shall ensure that all signalling during the lifetime of the dialogue is sent over the same flow (source IP and Port/destination IP and Port) as the dialogue initiating request.

NOTE 3a – The suggested way to ensure all signalling is sent over the same flow is to form a flow identifier token in the same way that a P-CSCF would form this for the Path header and insert this flow identifier token in the user portion of the URI used in the Record-Route header field value.

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 3581 [56A] and 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;

5) in case the request was received without signalling security, then check if the Via header contains the rport parameter with no value. If present, then the P-CSCF shall set the value of the parameter to the source port of the request as defined in RFC 3581 [56A];

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; and

2) if the received request was protected by a security association or TLS session, remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request;

3) in case the request was received without signalling security, then check if the Via header contains the rport parameter with no value. If present, then the P-CSCF shall set the value of the parameter to the source port of the request as defined in RFC 3581 [56A];

before forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26], the P-CSCF shall ensure that all signalling during the lifetime of the dialogue is sent over the same flow (source IP and Port/destination IP and Port) as the dialogue initiating request.

NOTE 4 – The suggested way to ensure all signalling is sent over the same flow is to form a flow identifier token in the same way that a P-CSCF would form this for the Path header and insert this flow identifier token in the user portion of the URI used in the Record-Route header field value.

When the P-CSCF receives from the UE an initial request or a target refresh request for a dialogue, and a Service-Route header list does not exist for the initiator of the request, the P-CSCF shall:

– reject the request with a 400 (Bad Request) response or silently discard the request; or

– continue with the procedures below, if it is a SUBSCRIBE request for the ua-profile event package and local policy allows such requests prior to registration:

1) add its own address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF in accordance with the procedures of RFC 3261 [26], and either:

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

b) the P-CSCF IP address;

2) in case the request was received without signalling security, then check if the Via header contains the rport parameter with no value. If present, then the P-CSCF shall set the value of the parameter to the source port of the request as defined in RFC 3581 [56A];

3) 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;

4) determine the I-CSCF of the home network and forward the request to that I-CSCF while ensuring that all signalling during the lifetime of the dialogue is sent over the same flow (source IP and Port/destination IP and Port) as the dialogue initiating request. If the selected I-CSCF does not respond to the request and its retransmissions by the P-CSCF, or sends back a 3xx response or 480 (Temporarily Unavailable) response to the request, then the P-CSCF shall select a new I-CSCF and forward the original request. If the P-CSCF fails to forward the request to any I-CSCF, 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].

NOTE 5 – The list of the I-CSCFs may be either obtained as specified in RFC 3263 [27A] or provisioned in the P-CSCF.

NOTE 6 – The suggested way to ensure all signalling is sent over the same flow is to form a flow identifier token in the same way that a P-CSCF would form this for the Path header and insert this flow identifier token in the user portion of the URI used in the Record-Route header field value.

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;

2a) if a security association does not exist, add its own SIP URI to the top of the received list of Record-Route headers in a format that contains the FQDN or IP address of the P-CSCF, save the list, and skip the execution of step 3;

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 ~~the comp parameter in accordance with the procedures of RFC 3486 [55], and~~ the protected server port number of the security association or TLS session established from the UE to the P-CSCF and either:

a) the P-CSCF FQDN that resolves to the IP address of the security association or TLS session established from the UE to the P-CSCF; or

b) the P-CSCF IP address of the security association or TLS session established from the

UE to the P-CSCF;

3a) if a security association does not exist, add its own address to the top of the received list of Via headers in a format that contains the FQDN or IP address of the P-CSCF, save the list, and skip the execution of step 4;

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 ~~the comp parameter in accordance with the procedures of RFC 3486 [55], and~~ the protected server port number of the security association or TLS session established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association or TLS session established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association or TLS session established from the UE to the P-CSCF;

NOTE 1 – For IPsec, t~~T~~he 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~~ITU-T J.366.7 [~~19~~98].

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) if a security association or TLS session exists, 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].

If secure signalling is not being used, the P-CSCF shall forward the request to the terminating UE over the flow identified by the flow identifier token as defined in RFC 5626 [86].

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

1) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with the value saved from the P-Called-Party-ID header that was received in the request if the response was protected by a security association or TLS session;

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

   a) discard the response; or

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

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

   a) discard the response; or

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

   If the verification is successful, the P-CSCF shall rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;

4) store the dialog ID and associate it with the private user identity and public user identity involved in the session; and

5) if the response corresponds to an INVITE request, save the Contact, To, From and Record-Route header field value received in the response such that the P-CSCF is able to release

the session if needed;

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

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

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

   a) discard the response; or

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

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

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

0) if a security association does not exist, add its own address to the top of the received list of Via headers in a format that contains the FQDN or IP address of the P-CSCF, save the list, and skip the execution of step 1;

1) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains ~~the comp parameter in accordance with the procedures of RFC 3486 [55], and~~ the protected server port number of the security association or TLS session established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association or TLS session established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association or TLS session established from the UE to the P-CSCF;

NOTE 2 – For IPsec, t~~T~~he 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~~ITU-T J.366.7 [~~19~~98].

1A) if a security association does not exist, add its own SIP URI to the top of the received list of Record-Route headers in a format that contains the FQDN or IP address of the P-CSCF, save the list, and skip the execution of step 2;

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 ~~the comp parameter in accordance with the procedures of RFC 3486 [55], and~~ the protected server port number of the security association or TLS session established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association or TLS session established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association or TLS session established from the UE to the P-CSCF; 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].

If secure signalling is not being used, the P-CSCF shall forward the request to the terminating UE over the flow identified by the flow identifier token as defined in RFC 5626 [86].

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

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

   a) discard the response; or

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

2) rewrite the port number of its own Record-Route entry to the same value as for the response to the initial request for the dialog if a security association or TLS session exists, 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) rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party if a security association or TLS session exists, and remove the comp parameter;

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

When the P-CSCF receives, destined for the UE, a request for a standalone transaction, or a request for an unknown method (that does not relate to an existing dialog), prior to forwarding the request, the P-CSCF shall:

0) if a security association does not exist, add its own address to the top of the received list of Via headers in a format that contains the FQDN or IP address of the P-CSCF, save the list, and skip the execution of step 1;

1) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains ~~the comp parameter in accordance with the procedures of RFC 3486 [55], and~~ the protected server port number of the security association or TLS session established from the UE to the P-CSCF and either:

   a) the P-CSCF FQDN that resolves to the IP address of the security association or TLS session established from the UE to the P-CSCF; or

   b) the P-CSCF IP address of the security association or TLS session established from the UE to the P-CSCF;

NOTE 4 – For IPsec, t~~T~~he 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~~ITU-T J.366.7 [~~19~~98].

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) if a security association or TLS session exists, 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 if the response was protected by a security association or TLS session;

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:

0) if a security association does not exist, add its own address to the top of the received list of Via headers in a format that contains the FQDN or IP address of the P-CSCF, save the list, and skip the execution of step 1;

1) add its own address to the top of the received list of Via header and save the list The P-CSCF Via header entry is built in a format that contains ~~the comp parameter in accordance with the procedures of RFC 3486 [55], and~~ the protected server port number of the security association or TLS session established from the UE to the P-CSCF and either:

a) the P-CSCF FQDN that resolves to the IP address of the security association or TLS session established from the UE to the P-CSCF; or

b) the P-CSCF IP address of the security association or TLS session established from the UE to the P-CSCF;

NOTE 5 – For IPsec, t~~T~~he 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~~ITU-T J.366.7 [~~19~~98].

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].

If secure signalling is not being used, the P-CSCF shall forward the request to the terminating UE over the flow identified by the flow identifier token as defined in RFC 5626 [86].

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].

• • •

5.2.8.1.4 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 or TLS session 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 that the session has been terminated.

• • •

5.2.11 Void

5.2.12 STUN Server

The P-CSCF shall also support the requirements for a STUN server that sits on the same signalling port that is used for SIP. This subsumes requirements defined by RFC 5389 [83].

• • •

5.4.1.2.1 Unprotected REGISTER

NOTE 0 – An unprotected REGISTER is a register request sent from the UE to the P-CSCF without any integrity protection or mutual authentication. When the "integrity protected" parameter is present in the Authorization header, it will be set to "no". In the case where a UE has established a server side authenticated TLS session with the P-CSCF, but has not yet authenticated, the REGISTER is considered unprotected and the P-CSCF will not set the "integrity protected" parameter to "yes".

NOTE 1 – Any REGISTER request sent unprotected by the UE is considered to be an initial registration, unless signalling security is disabled (between the UE and P-CSCF). 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 unless signalling security is disabled.

NOTE 2 – A REGISTER with Expires header value equal to zero should always be received protected unless signalling security is disabled. 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", for an already registered public user identity linked to the same private user identity and contact information (e.g., UE re-registers or de-registers over the same network with signalling security disabled), the S-CSCF shall skip the remaining steps in this subclause and execute the steps in subclause 5.4.1.2.2 as though "integrity-protected" is set to "yes".

NOTE 2a – When following the steps in subclause 5.4.1.2.2 for an unprotected REGISTER, the S-CSCF should require all REGISTER messages to be authenticated (even if the user has previously authenticated).

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;

1a) check if authentication is currently ongoing for the user (i.e., timer reg-await-auth is running), and if it is, the S-CSCF shall skip the remaining steps in this subclause and execute the steps in subclause 5.4.1.2.2 for the case where the timer reg-await-auth is running (for a protected REGISTER);

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~~ITU-T J.366.7 [~~19~~98].

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;

if the digest algorithm is AKAv1-MD5:

- 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);

If the digest algorithm is MD5, refer to ITU-T J.366.7 [98] for WWW-Authenticate header contents.

6) for an AKAv1-MD5 based digest, store the RAND parameter used in the 401 (~~Unathorized~~Unauthorized) response for future use in case of a resynchronisation. If a stored RAND already exists in the S-CSCF, the S-CSCF shall overwrite the stored RAND with the RAND used in the most recent 401 (Unauthorized) response;

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

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

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

5.4.1.2.2 Protected REGISTER

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

In the case that there is no authentication currently ongoing for this user (i.e., no timer reg-await-auth is running):

1) check if the user needs to be reauthenticated.

   The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for REGISTER requests received without the "integrity-protected" parameter in the Authorization header set to "yes".

   If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph; and

2) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall check whether the public user identity received in the To header is already registered. If it is not registered, the S-CSCF shall proceed beginning with step 5 below. Otherwise, the S-CSCF shall proceed beginning with step 6 below.

In the case that a timer reg-await-auth is running for this user the S-CSCF shall:

1) check if the Call-ID of the request matches with the Call-ID of the 401 (Unauthorized) response which carried the last challenge. The S-CSCF shall only proceed further if the Call-IDs match.

2) stop timer reg-await-auth;

3) check whether an Authorization header is included, containing:

   a) the private user identity of the user in the username field;

   b) the algorithm in the algorithm field which matches the algorithm sent in the authentication challenge~~which is AKAv1-MD5 in the algorithm field~~; ~~and~~

   c) the authentication challenge response needed for the authentication procedure in the response field~~.~~; and

   d) in the case of the MD5 algorithm, any other required fields as specified in ITU-T J.366.7 [98].

   The S-CSCF shall only proceed with the following steps in this paragraph if the authentication challenge response was included;

4) check whether the received authentication challenge response and the expected authentication challenge response~~ (calculated by the S-CSCF using XRES and other parameters as described in RFC 3310 [49])~~ match:

   a) For an AKAv1-MD5 based challenge, the expected authentication challenge response is calculated by the S-CSCF using XRES and other parameters as described in RFC 3310 [49] (t~~T~~he XRES parameter was received from the HSS as part of the Authentication Vector).

   b) For a SIP digest based (e.g., MD5) challenge, the expected authentication challenge response is calculated by the S-CSCF as described in ITU-T J.366.7 [98]. The S-CSCF also uses user credentials obtained (previously) from the HSS to calculate the expected challenge response.

   The S-CSCF shall only proceed with the following steps if the challenge response received from the UE and the expected response calculated by the S-CSCF match;

5) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.228 [14], store the following information in the local data:

a) the list of public user identities associated to the ~~the~~ public user identity under registration, including the own public user identity under registration and the implicitly registered due to the received REGISTER request. Each public user identity is identified as either barred or non-barred; and,

b) all the service profile(s) corresponding to the public user identities being registered (explicitly or implicitly), including initial Filter Criteria (the initial Filter Criteria for the Registered and common parts is stored and the ~~unregisterd~~unregistered part is retained for possible use later – in the case of the S-CSCF is retained if the user becomes unregistered);

NOTE 1 – There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same user's subscription may belong to different service profiles.

6) bind to each non-barred registered public user identity all registered contact information including all header parameters contained in the Contact header (with the exception of the 'gruu' header parameter which shall be ignored if present) and all associated URI parameters and store information for future use;

NOTE 2 – There might be more than one contact information available for one public user identity.

NOTE 3 – The barred public user identities are not bound to the contact information.

7) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4 – If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

8) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;

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

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

a) the list of received Path headers;

b) a P-Associated-URI header containing the list of public user identities that are associated to the public user identity under registration. The first URI in the list of public user identities supplied by the HSS to the S-CSCF will indicate the default public user identity to be used by the S-CSCF. The public user identity indicated as the default public user identity must be an already registered public user identity. The S-CSCF shall place the default public user identity as a first entry in the list of URIs present in the P-Associated-URI header. The default public user identity will be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header, as described in subclause 5.2.6.3. The S-CSCF shall not add a barred public user identity to the list of URIs in the P-Associated-URI header;

c) a Service-Route header containing:

– the SIP URI identifying the S-CSCF containing an indication that requests routed via the service route (i.e., from the P-CSCF to the S-CSCF) are treated as for the mobile-originating case. This indication may e.g., be in a URI parameter, a character string in the user part of the URI or be a port number in the URI; and,

– if network topology hiding is required a SIP URI identifying an I-CSCF(THIG) as the topmost entry;

d) a P-Charging-Function-Addresses header containing the values received from the HSS if the P-CSCF is in the same network as the S-CSCF. It can be determined if the P-CSCF is in the same network as the S-CSCF by the contents of the P-Visited-Network-ID header field included in the REGISTER request; ~~and~~

e) a Contact header listing all contact addresses for this public user identity~~.~~, and including all saved header and URI parameters; and

f) if the REGISTER request contained a Required or Supported header containing the value 'gruu', then gruus shall be included in the Contact header as follows:

– for each contact address in the contact header that has a +sip.instance header parameter, add a 'gruu' header parameter;

– the value of the 'gruu' parameter shall consist of the public user identity in the To header, with the addition of two URI parameters: an 'opaque' parameter with value identical to that of the +sip.instance contact header parameter, and a 'gruu' parameter with no value. Appropriate escaping shall be applied to the values to preserve valid syntax of the response.

NOTE 4a – In step f) parameters are added to the URI. URI parameters are part of the URI, and are distinguished from header parameters which may be part of a header that contains a URI. The 'gruu' parameter is valid as both a header parameter and a URI parameter. The two usages have different meanings: the URI parameter indicates that the URI is a GRUU, while the header parameter is used, with a value, to return a GRUU. The following is an example of a Contact header that could appear in the response to a REGISTER request, including an assigned gruu:

Contact: <sip:xyz@192.0.2.1>; +sip.instance="<urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6>"; gruu="sip:callee@example.com;gruu;opaque=urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6"

NOTE 5 – There might be other contact addresses available, that other UEs have registered for the same public user identity.

11) send the so created 200 (OK) response to the UE;

12) 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,

NOTE 6 – If this registration is a reregistration, the Filter Criteria already exists in the local data.

13) handle the user as registered for the duration indicated in the Expires header.

5.4.1.2.3 Abnormal cases

In the case that the REGISTER request, that contains the authentication challenge response from the UE does not match with the expected REGISTER request (e.g., wrong Call-Id or authentication challenge response) and the request has the "integrity-protected" parameter in the Authorization header set to "yes", the S-CSCF shall:

– send a 403 (Forbidden) response to the UE. The S-CSCF shall consider this authentication attempt as failed. The S-CSCF shall not update the registration state of the subscriber~~.~~, or

– rechallenge the user by issuing a 401 (Unauthorized) response including a challenge as per the procedures described in ITU-T J.366.7 [98].

NOTE 1 – If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request, that contains the authentication challenge response from the UE, does not match with the expected REGISTER request (e.g., wrong Call-Id or authentication challenge response) and the request does not contain an "integrity-protected" parameter or contains the "integrity-protected" parameter in the Authorization header set to "no", the S-CSCF shall:

- send a 403 (Forbidden) response to the UE. The S-CSCF shall consider this authentication attempt as failed. The S-CSCF shall not update the registration state of the subscriber;
- rechallenge the user by issuing a 401 (Unauthorized) response including a challenge as per the procedures described in ITU-T J.366.7 [98].

NOTE 1a – If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request, which was supposed to carry the response to the challenge, contains no authentication challenge response and in the case of AKAv1-MD5 digest challenge no AUTS parameters indicating that the MAC parameter was invalid in the challenge, the S-CSCF shall:

- respond with a 403 (Forbidden) response to the UE. The S-CSCF shall not update the registration state of the subscriber.

NOTE 2 – If the UE was registered before, it stays registered until the registration expiration time expires.

In the case that the REGISTER request from the UE containing an authentication challenge response for AKAv1-MD5 indicates that the authentication challenge was invalid (contains the AUTS parameter indicating this), the S-CSCF will fetch new authentication vectors from the HSS. In order to indicate a resynchronisation, the S-CSCF shall include the AUTS received from the UE and the stored RAND, when fetching the new authentication vectors. On receipt of the new authentication vectors from the HSS, the S-CSCF shall either:

- send a 401 (Unauthorized) response to initiate a further authentication attempt, using these new vectors; or
- respond with a 403 (Forbidden) response if the authentication attempt is to be abandoned. The S-CSCF shall not update the registration state of the subscriber.

NOTE 3 – If the UE was registered before, it stays registered until the registration expiration time expires.

NOTE 4 – Since the UE responds only to two consecutive invalid challenges, the S-CSCF will send a 401 (Unauthorized) response that contains a new challenge only twice.

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, the S-CSCF may initiate network-initiated deregistration procedure based on the information in the Filter Criteria. 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 with the highest "q" value;
- 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.

NOTE 5 – If the timer reg-await-auth expires, the S-CSCF will consider the authentication to have failed. If the public user identity was already registered, the S-CSCF will leave it as registered described in ~~3GPP TS 33.203~~ITU-T J.366.7 [~~19~~98].

In the case that the S-CSCF receives a REGISTER request with the "integrity-protected" parameter in the Authorization header set to "yes", for which the public user identity received in the To header and the private user identity received in the Authorization header of the REGISTER request do not match to any registered user at this S-CSCF, the S-CSCF shall:

– respond with a 500 (Server Internal Error) response to the UE.

5.4.1.2.4 Support for outbound routing through NATs

The S-CSCF shall follow the requirements defined in RFC 5626 [86].

5.4.1.3 Authentication and reauthentication

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

5.4.1.4 User-initiated deregistration

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

– check whether the "integrity-protected" parameter in the Authorization header field set to "yes", indicating that the REGISTER request was received integrity protected. If the "integrity-protected" parameter is not present or if it is set to "no" the S-CSCF shall ensure authentication is performed (if necessary) as described in subclause 5.4.1.2.1 (and consequently subclause 5.4.1.2.2)~~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 used identities by applying the steps listed in subclause 5.4.5.1.2;

– if this public used 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 used 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 the "integrity protected" parameter was set to the value "no", the S-CSCF shall apply the procedures described in subclause 5.4.1.2.1.

On completion of the above procedures in this subclause and of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.228 [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).

5.4.1.5 Network-initiated deregistration

NOTE 1 – A network-initiated deregistration event that occurs at the S-CSCF may be received from the HSS or may be an internal event in the S-CSCF.

Prior to initiating the network-initiated deregistration for the only currently registered public user identity and its associated set of implicitly registered public user identities that have been registered with the same contact (i.e., no other public user identity is registered with this contact) while there are still active multimedia sessions belonging to this contact, the S-CSCF shall release only the multimedia sessions belonging to this contact as described in the following paragraph. The multimedia sessions for the same public user identity, if registered with another contact remain unchanged.

Prior to initiating the network-initiated deregistration while there are still active multimedia sessions that are associated with this user and contact, the S-CSCF shall release none, some or all of these multimedia sessions by applying the steps listed in subclause 5.4.5.1.2 under the following conditions:

– when the S-CSCF does not expect the UE to reregister (i.e., S-CSCF will set the event attribute within the <contact> element to "rejected" for the NOTIFY request, as described below), the S-CSCF shall release all sessions that are associated with the public user identities being deregistered, which includes the implicitly registered public user identities~~.~~;

– when the S-CSCF expects the UE to reregister (i.e., S-CSCF will set the event attribute within the <contact> element to "deactivated" for the NOTIFY request, as described below), the S-CSCF shall only release sessions that currently include the user, where the session was initiated with the one of the public user identities being deregistered, which includes the implicitly registered public user identities.

When a network-initiated deregistration event occurs for one or more public user identities that are bound to one or more contacts, the S-CSCF shall send a NOTIFY request to all subscribers that have subscribed to the respective reg event package. For each NOTIFY request, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

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

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

   b) if the public user identity:

      i) has been deregistered then:

         – set the state attribute within the <registration> element to "terminated";

         – set the state attribute within the <contact> element to "terminated"; and

         – set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

      ii) has been kept registered then:

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

         II) set the state attribute within the <contact> element to:

            – for the contact address to be removed set the state attribute within the <contact> element to "terminated", and event attribute element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

            – for the contact ~~address~~ addresses which remain unchanged, if any, ~~leave~~

~~the <contact> element unmodified~~set the <gruu> sub-element of the <contact> element as specified in clause 5.4.2.1.2; and

NOTE 2 – There might be more than one contact information available for one public user identity. When deregistering this UE, the S-CSCF will only modify the <contact> elements that were originally registered by this UE using its private user identity. The <contact> elements of the same public user ~~identitity~~identity, if registered by another UE using different private user identities remain unchanged.

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

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

Also, the S-CSCF shall send a third-party REGISTER request, as described in subclause 5.4.1.7, to each AS that matches the Filter Criteria from the HSS as if a equivalent REGISTER request had been received from the user deregistering that public user identity, or combination of public user identities.

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

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

5.4.1.6 Network-initiated reauthentication

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

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

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns:

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

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

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

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

   e) set the event attribute within each <contact> element 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

g) set the <gruu> sub-element within each <contact> element as specified in clause 5.4.2.1.2.

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 ~~identitity~~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).

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.

• • •

5.4.2.1.1 Subscription to the event providing registration state

When an incoming SUBSCRIBE request addressed to S-CSCF arrives containing the Event header with the reg event package, the S-CSCF shall:

0) follow the procedures in clause 5.4.8 to challenge the request if needed;

1) check if, based on the local policy, the request was generated by a subscriber who is authorised to subscribe to the registration state of this particular user. The authorized subscribers include:

   – all public user identities this particular user owns, that the S-CSCF is aware of, and which are not-barred;

   – all the entities identified by the Path header (i.e., the P-CSCF to which this user is attached to); and

   – all the ASs listed in the initial filter criteria and not belonging to third-party providers.

NOTE 1 – The S-CSCF finds the identity for authentication of the subscription in the P-Asserted-Identity header received in the SUBSCRIBE request.

2) generate a 2xx response acknowledging the SUBSCRIBE request and indicating that the authorised subscription was successful as described in RFC 3680 [43]. The S-CSCF shall populate the header fields as follows:

   – an Expires header, set to either the same or a decreased value as the Expires header in SUBSCRIBE request.

The S-CSCF may set the Contact header to an identifier uniquely associated with the SUBSCRIBE request and generated within the S-CSCF, that may help the S-CSCF to correlate refreshes for the SUBSCRIBE.

NOTE 2 – The S-CSCF could use such unique identifiers to distinguish between UEs, when two or more users, holding a shared subscription, register under the same public user identity.

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

5.4.2.1.2 Notification about registration state

For each NOTIFY request on all dialogs which have been established due to subscription to the reg event package of that user, the S-CSCF shall:

1) set the Request-URI and Route header to the saved route information during subscription;

2) set the Event header to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

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

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

   aa) the S-CSCF shall add gruu information as follows:

   – if the aor attribute of the <registration> element contains a sip or sips URI, then:

     • for each contact address that contains a +sip.instance header parameter, include a <gruu> sub-element within the corresponding <contact> element;

     • the contents of the <gruu> sub-element shall consist of the aor attribute of the <registration> element, with the addition of two gruu parameters: an 'opaque' URI parameter with value identical to that of the +sip.instance contact header parameter, and a 'gruu' parameter with no value. Appropriate escaping shall be applied to the values to preserve valid syntax of the resulting URI;

   – if the aor attribute of the <registration> element contains a tel URI:

     • determine if there is a <registration> element whose aor attribute is a sip or sips URI equivalent to the tel URI of this element. A sip or sips URI is equivalent to the tel URI if:

       ○ the user part of the sip or sips URI equals the content of the tel URI according to the rules of comparison for tel URIs;

       ○ the sip or sips URI contains a 'user=phone' URI parameter;

       ○ the two URIs share the same service profile;

       ○ if there is an equivalent element, then include a copy of the <gruu> sub-element from that;

   b) if the public user identity:

   I) has been deregistered (i.e., no active contact left) then:

     – set the state attribute within the <registration> element to "terminated";

     – set the state attribute within each <contact> element to "terminated"; and

     – set the event attribute within each <contact> element to "deactivated", "expired", "unregistered", "rejected" or "probation" according to RFC 3680 [43].

     If the public user identity has been deregistered and the deregistration has already been indicated in the NOTIFY request, and no new registration has occurred, its <registration> element shall not be included in the subsequent NOTIFY requests; or

   II) has been registered then:

     – set the <unknown-param> element to any additional header parameters contained in the contact header of the REGISTER request according to RFC 3680 [43];

     – set the state attribute within the <registration> element to "active", if not already set to "active", otherwise leave it unchanged; and either:

     – for the contact address to be registered: set the state attribute within the <contact> element to "active"; and set the event attribute within the <contact>

element to "registered"; or

- for the contact address which remain unchanged, if any, leave the <contact> element unmodified; or

III) has been automatically registered, and have not been previously automatically registered:

- set the <unknown-param> element to any additional header parameters contained in the contact header of the ~~originsl~~original REGISTER request according to RFC 3680 [43];
- set the state attribute within the <registration> element to "active";
- set the state attribute within the <contact> element to "active"; and
- set the event attribute within the <contact> element to "created"; and

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

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

EXAMPLE: If sip:user1_public1@home1.net is registered, the public user identity sip:user1_public2@home1.net can automatically be registered. Therefore the entries in the body of the NOTIFY request look like:

```
<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
             version="0" state="full">
  <registration aor="sip:user1_public1@home1.net" id="as9"
                state="active">
    <contact id="76" state="active" event="registered">
           <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
           <unknown-param name="audio"/>
    </contact>
  </registration>
  <registration aor="sip:user1_public2@home1.net" id="as10"
                state="active">
    <contact id="86" state="active" event="created">
           <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
           <unknown-param name="audio"/>
    </contact>
  </registration>
</reginfo>
```

When sending a final NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e., all public user identities have been deregistered or expired), the S-CSCF shall also terminate the subscription to the registration event package by setting the Subscription-State header to the value of "terminated".

When all UE's contact addresses have been deregistered ~~(i.e.,there~~ (i.e., there is no <contact> element set to "active" for this UE), the S-CSCF shall consider subscription to the reg event package belonging to the UE cancelled (i.e., as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

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

•••

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, and the request does not contain a P-Asserted-Identity header, the S-CSCF shall perform the steps in clause 5.4.8 to challenge the request, if necessary.

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.

0) determine the public user identity of the request initiator by the P-Asserted-Identity header, if present. If the P-Asserted-Identity header is not present, then the P-Preferred-Identity header (if present) or the From header (if the P-Preferred-Identity header is absent) is used as the public user identity of the initiator;

1) determine whether the public user identity of the request ~~contains~~ initiator is 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,~~. If so, 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 of the request initiator ~~in the P-Asserted-Identity header~~ in the priority order as described in 3GPP TS 23.218 [5], and if it does, the S-CSCF shall:

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

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

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

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

6) if there is no original dialog identifier present in the topmost Route header of the incoming request insert an 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 (if present), 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;

a) Furthermore, if the outgoing Request-URI is a tel URI and the translation of the tel URI to a SIP URI fails, and if the S-CSCF supports number portability and is configured to populate number portability parameters in the tel URI, then:

– if the tel URI does not include a "npdi" parameter, then the S-CSCF shall determine if the called number is ported. The means to determine that the called number is ported is outside the scope of this document. If the number is ported, then the S-CSCF shall include the "rn" parameter in the tel URI in the Request-URI to identify the ported-to routing number, and add an "npdi" parameter to indicate that the local number portability database dip has been performed (as described in RFC 4694 [91]);

– if the tel URI includes a "npdi" parameter, the S-CSCF shall not update the tel URI "rn" or "npdi" parameter;

NOTE 2a – In the case of a ported number to a peer network, local policy may dictate that call is routed to the PSTN.

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 address is of an IP address type other than the IP address type used in the IM CN subsystem, then the S-CSCF shall forward the request to the IMS-ALG if the IM CN subsytem supports interworking to networks with different IP address type;

11) if network hiding is needed due to local policy, put the address of the I-CSCF(THIG) to the topmost route header;

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

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

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

– the contact address contains 'gruu' and 'opaque' URI parameters; and

– the contact address with those parameters removed compares equal to the public user identity of the request initiator or to any other public user identity in an implicit registration set with the request initiator;

b) determine the need to record-route for other reasons:

– if the request is routed to an AS which is part of the trust domain, the S-CSCF 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.

c) if gruu processing is required, or there is a need to record-route for other reasons: the S-CSCF shall create a Record-Route header containing its own SIP URI;

d) if gruu processing is required, the S-CSCF save an indication that gruu-routing is to be performed for in-dialog requests that reach the S-CSCF because of the Record-Route header added in step c);

e) if gruu processing is required, the S-CSCF shall follow the procedures in RFC 5627 [87] to determine and save the contact or reg-id over which the response has been received;

NOTE 3a – The manner of representing the gruu-routing indication and chosen contact or reg-id is a private matter for the S-CSCF. The indication is used during termination processing of in-dialog requests to cause the S-CSCF to replace a request-URI containing a GRUU with the corresponding registered contact address. They may be saved using values in the Record-Route header, or in dialog state.

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.

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 other non-2xx 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.

NOTE 4 – The P-Asserted-Identity header would normally only be expected in 1xx or 2xx responses.

NOTE 5 – The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3325 [34].

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

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

When the S-CSCF, upon sending an initial INVITE request that includes an IP~~v6~~ address in the SDP offer (in "c=" parameter), receives an error response indicating that the ~~the~~ IP address type ~~used in the IM CN subsystem~~ 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 IMS-ALG; 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 a 1xx or 2xx response to the target refresh request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed.

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

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

2) in case the request is routed towards the destination user (Request-URI) or 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.

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) 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;

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 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 and skip the following steps.

4a) ~~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;

7a) in the case there are no Route headers in the request, create a list of potential next hop destinations as follows:

a) if the request URI is a gruu (i.e., the request URI contains 'gruu' and 'opaque' URI parameters), then the list of potential destinations is determined by following the procedures of RFC 5627 [87], using the value of the 'opaque' parameter as the instance ID;

b) if the request URI is not a GRUU, then set the list of potential destinations to all the registered contacts saved as described in subclause 5.4.1.2;

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

NOTE 1a – This may eliminate entries and reorder the list.

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) void~~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~~ the next hop destination from the list of next hop destinations determined above. If there is more than one ~~contact address saved for the destination public user identity~~next hop destination, 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;

   – In case that no no-next hop destination is chosen, the S-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) and terminate these procedures.

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

d) insert a P-Called-Party-ID SIP header field including the Request-URI received in the request, derived by starting with the Request-URI and removing 'gruu' and 'opaque' URI parameters, if both are present;

Note that in 9 b), when the S-CSCF proxies a request to a particular contact, additional rules defined in RFC 5626 [86] also apply:

– The S-CSCF shall not populate the target set with more than one contact with the same AOR and instance-id at a time. If a request for a particular AOR and instance-id fails with a 410 response, the S-CSCF shall replace the failed branch with another target with the same AOR and instance-id, but a different reg-id.

– If two bindings have the same instance-id and reg-id, it should prefer the contact that was most recently updated.

Note that if the request URI is a GRUU, the S-CSCF will only select contacts with the AOR and instance-id associated with the GRUU. The rules above still apply to a GRUU. This allows a request routed to a GRUU to first try one of the flows to a UA, then if that fails, try another flow to the same UA instance.

e) build the Route header field with values from the list of preloaded routes for the next hop destination saved during registration or re-registration, as described in subclause 5.4.1.2;

f) save the request URI and the total number of Record-Route headers as part of the dialog request state;

NOTE 1b – For each initial dialog request terminated at a served user two pieces of state are maintained to assist in processing GRUUs: the chosen contact address to which the request is routed; and the position of an entry for the S-CSCF in the Record-Route header that will be responsible for gruu translation, if needed. (The position is the number of entries in the list before the entry was added. The entry will be added in step 12 below.) The S-CSCF may record-route multiple times, but only one of those (the last) will be responsible for gruu translation at the terminating end.

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;

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].

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 4a; 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 all the procedures described ~~in the steps 1, 2 and, 3 in the~~ above in the paragraph beginning with: ~~(~~when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction.~~)and3) 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 a 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), it shall:

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

2) insert 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)~~.~~;

5) determine the need for gruu processing:

gruu processing is required if:

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

b) the contact address in the response contains 'gruu' and 'opaque' URI parameters; and

c) the contact address with those parameters removed compares equal to any URI in the P-Asserted-Identity header of the response or to any other public user identity in an implicit registration set with it;

6) if gruu processing is required, the S-CSCF shall:

a) save an indication that gruu-routing is to be performed for in-dialog requests that reach the S-CSCF because of the Record-Route header added in step 12 above;

b) follow the procedures in RFC 5627 [87] to determine and save the contact or reg-id over which the response has been received.

NOTE 3 – The manner of representing the gruu-routing indication and chosen contact or reg-id is a private matter for the S-CSCF. Both are used during termination processing of in-dialog requests. They may be saved using values in the Record-Route header, or in dialog state.

NOTE 4 – There may be several responses returned for a single request, and the decision to insert or modify the Record-Route must be applied to each. But a response may also return to the S-CSCF multiple times as it is routed back through Application Servers. The S-CSCF should take this into account when carrying out step 6 – the information should be stored only once.

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;

1a) if the topmost Route header in the incoming request contains an indication that gruu-routing is to be performed for in-dialog requests, and the request URI is not the target contact for the dialog, then return a response of 400 (Bad Request) that may include a Warning header containing the warn-code 399;

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;

2a) if the topmost Route header in the incoming request contained an indication that gruu-routing is to be performed for in-dialog requests:

   - translate the gruu and replace the request-URI following the procedures in RFC 5627 [87], using the value of the 'opaque' parameter as the instance ID and the contact or reg-id saved at the time of dialog establishment;
   - if a contact was not selected, return a response of 480 (Temporarily Unavailable);

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

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

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

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

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

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

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

1a) if the topmost Route header in the incoming request contained an indication that gruu-routing is to be performed for in-dialog requests:

   - translate the gruu and replace the request-URI following the procedures in RFC 5627 [87], using the value of the 'opaque' parameter as the instance ID and the contact or reg-id saved at the time of dialog establishment;
   - if a contact was not selected, return a response of 480 (Temporarily Unavailable).

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

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

5.4.3.4 Original dialog identifier

…

5.4.8 General authentication procedures for all SIP request methods initiated by the UE excluding REGISTER

When the S-CSCF receives from the UE a request (excluding REGISTER) that does not contain a P-Asserted-Identity header, the S-CSCF shall perform the following steps:

1) the S-CSCF shall identify the initiator of the request by the public user identity contained in the P-Preferred-Identity header if present, or the From header otherwise;

2) if the public user identity does not match one of the registered public user identities, the S-CSCF shall:

   a) reject the request with a 400 (Bad Request) response or silently discard the request; or

   b) continue with the execution of steps 3 onward;

3) if the request does not contain credentials, the S-CSCF shall:

   a) challenge the initiator by issuing a 401 (Unauthorized) response including a challenge as per procedures described in ITU-T J.366.7 [98]; or

   b) consider the identity of the user unverified and the request unauthenticated;

4) if the request contains credentials and the credentials are correct, the S-CSCF shall consider the identity of the user verified and the request authenticated. The S-CSCF shall insert a P-Asserted-Identity header with a value representing the initiator of the request;

5) if the request contains credentials but the credentials are not correct, the S-CSCF shall:

   a) rechallenge the user by issuing a 401 (Unauthorized) response including a challenge as per procedures described in ITU-T J.366.7 [98]; or

   b) reject the request by issuing a 403 (Forbidden) response; or

   c) consider the identity of the user unverified and the request unauthenticated;

6) if the S-CSCF considers the identity of the user unverified and the request unauthenticated, the S-CSCF shall:

   a) reject the request with a 400 (Bad Request) response or silently discard the request; or

   b) continue with the execution of step 7;

   NOTE – Local policy may allow unverified users to initiate certain non-REGISTER requests.

7) the S-CSCF shall remove the P-Preferred-Identity header if present prior to forwarding the request, and continue with the procedures below.

5.5 Procedures at the MGCF

…

5.5.3.1.1 Calls originated from circuit-switched networks

When the MGCF receives an indication of an incoming call from a circuit-switched network, the MGCF shall:

- generate and send an INVITE request to I-CSCF:
- set the Request-URI to the "tel" format using an E.164 address;
- set the Supported header to "100rel" if reliability of provisional responses in SIP is used (see RFC 3312 [30] as updated by RFC 4028 [64]);
- include an P-Asserted-Identity header, depending on corresponding information in the circuit-switched network;

- create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and
- insert an orig-ioi parameter into the P-Charging-Vector header. The orig-ioi parameter shall be set to a value that identifies the sending network in which the MGCF resides and the term-ioi parameter shall not be included.

When the MGCF receives a 1xx or 2xx response to an initial request for a dialog, the MGCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present. The term-ioi parameter identifies the sending network of the response message.

5.5.3.1.2 Calls terminating in circuit-switched networks

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

- store the value of the orig-ioi parameter received in the P-Charging-Vector header, if present. The orig-ioi parameter identifies the sending network of the request message;
- send 100 (Trying) response;
- after a matching codec is found or no codec is required at the MGW, send 183 "Session Progress" response:
  - set the Require header to the value of "100rel" if reliability of provisional responses in SIP is required;
  - store the values received in the P-Charging-Function-Addresses header;
  - store the value of the icid parameter received in the P-Charging-Vector header; and
  - insert a term-ioi parameter into the P-Charging-Vector header. The term-ioi parameter shall be set to a value that identifies the network in which the MGCF resides.

If a codec is required and the MGCF does not find an available matching codec at the MGW for the received initial INVITE request, the MGCF shall:

- send 503 (Service Unavailable) response if the type of codec was acceptable but none were available; or
- send 488 (Not Acceptable Here) response if the type of codec was not supported, and may include SDP in the message body to indicate the codecs supported by the MGCF/MGW.

5.5.3.2 Subsequent requests

5.5.3.2.1 Calls originating in circuit-switched networks

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

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

The MGCF shall send an UPDATE request when the following conditions are fulfilled:

- the MGCF supports UPDATE;
- the UE supports UPDATE as indicated in the Allow headers;
- conditions as specified in 3GPP TS 29.1~~5~~63 [11B]; and
- the MGCF receives 200 (OK) response to a PRACK request

•••

5.6.2 Session initiation transaction

When the BGCF receives an INVITE request, the BGCF shall forward the request either to an MGCF within its own network, or to another network containing an MGCF. The BGCF need not Record-Route the INVITE request. While the next entity may be a MGCF acting as a UA, the

BGCF shall not apply the procedures of RFC 3323 [33] relating to privacy. The BGCF shall store the values received in the P-Charging-Function-Addresses header. The BGCF shall store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header.

NOTE 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.

If the BGCF supports carrier routing parameters and is configured to populate the caller's preassigned carrier in the tel URI, and the preassigned carrier is required for this call, then the BGCF shall include the "cic" parameter in the tel URI identifying the preassigned carrier, plus the "dai" parameter (as described in the IPCablecom CMSS specification [96]) to identify how the "cic" parameter was obtained. The BGCF shall not add the "cic" parameter value in the tel URI if the parameter is already exists in the tel URI, or if the request URI is a freephone number.

NOTE 1a – Local policy should be able to control the interaction and precedence between routing on "cic" parameter versus routing based on "rn" parameter.

NOTE 1b – The means to configure the BGCF with the pre-assigned carrier is outside the scope of this document.

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.

5.7 Procedures at the Application Server (AS)

•••

5.7.2 Application Server (AS) acting as terminating UA, or redirect server

When acting as a terminating UA the AS shall behave as defined for a UE in subclause 5.1.4, with the exceptions identified in this subclause.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

An AS acting as redirect server shall propagate any received IM CN subsystem XML message body in the redirected message.

When an AS acting as a terminating UA generates a subsequent request that does not relate to an INVITE dialog, the AS shall insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

When an AS, acting as a terminating UA, terminates a dialog establishing request or target refresh request, if the contact address it includes in the response possesses the GRUU property (as specified in RFC 5627 [87]) then that contact address should include a 'gruu' URI parameter.

5.7.3 Application Server (AS) acting as originating UA

When acting as an originating UA the AS shall behave as defined for a UE in subclause 5.1.3, with the exceptions identified in this subclause.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

When an AS acting as an originating UA generates an initial request for a dialog or a request for a standalone transaction, the AS shall insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17]. The AS may retrieve CCF and/or ECF addresses from HSS on Sh interface.

When an AS acting as an originating UA generates a subsequent request that does not relate to an INVITE dialog, the AS shall insert a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

When an AS, acting as an originating UA, generates an initial request for a dialog or a target refresh request, if the contact address it includes in the request possesses the GRUU property (as specified in RFC 5627 [87]) then that contact address should include a 'gruu' URI parameter.

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

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

When sending an initial request on behalf of a PSI that is hosted by the AS, the AS shall insert a Route header pointing to an S-CSCF of the home network of the PSI, if:

– the AS is not able to resolve the next hop address by itself; or

– the operator policy requires it.

NOTE 1 – The address of the S-CSCF may be obtained by querying the HSS on the Sh interface or from static configuration.

When sending an initial request on behalf of a public user identity, the AS shall insert a Route header pointing to the S-CSCF where the public user identity on whose behalf the request is generated is registered or hosted (unregistered case).

NOTE 2 – The address of the S-CSCF may be obtained either from a previous request terminated by the AS, by querying the HSS on the Sh interface or from static configuration.

For the use of the P-Asserted-Identity by the AS, at least two cases exist:

a) any initial request for a dialog or request for a standalone transaction is generated as if it was originated by the UE on whose behalf the request is generated. In this case the AS shall insert a P-Asserted-Identity representing a public user identity of that UE. The AS shall append the "orig" parameter to the URI of the S-CSCF; and

b) any initial request for a dialog or request for a standalone transaction is generated by an AS supporting a service identified by a PSI. In this case the AS shall insert a P-Asserted-Identity containing the PSI of the AS. Also, the AS shall append the "orig" parameter to the URI of the S-CSCF.

Editor's Note: It needs to be specified that the AS can only add the P-Asserted-Identity when the AS is within the trust domain.

The AS can indicate privacy of the P-Asserted-Identity in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

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

NOTE 3 – The contents of the From header should not be relied upon to be modified by the network based on any privacy specified by the user either within the AS indication of privacy or by network subscription or network policy. Therefore the AS should include the value "Anonymous" whenever privacy is explicitly required.

Editor's note: Is there a need to specify any conditions for the AS choosing to indicate privacy that are generic to all originating AS, or all conditions service specific, and therefore out of the scope of 24.229.

5.7.4 Application Server (AS) acting as a SIP proxy

• • •

5.7.5.1 General

The AS performing 3rd party call control acts as a B2BUA. There are two kinds of 3rd party call control:

– Routeing B2BUA: an AS receives a request from the S-CSCF, terminates it and generates a new request, which is based on the received request.

– Initiating B2BUA: an AS initiates two requests, which are logically connected together at the AS, or an AS receives a request from the S-CSCF and initiates a new request that is logically connected but unrelated to the incoming request from the originating user (e.g., the P-Asserted-Identity of the incoming request is changed by the AS).

When the AS receives a terminated call and generates a new call, and dependent on whether the service allows the AS to change the P-Asserted-Identity for outgoing requests compared with the incoming request, the AS will select appropriate kind of 3rd party call control.

The B2BUA AS will internally map the message headers between the two dialogs that it manages. It is responsible for correlating the dialog identifiers and will decide when to simply translate a message from one dialog to the other, or when to perform other functions. These decisions are specific to each AS and are outside the scope of the present document.

The AS, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.

For standalone transactions, when the AS is acting as a Routeing B2BUA, the AS shall copy the remaining Route header(s) unchanged from the received request for a standalone ~~transation~~transaction to the new request for a standalone transaction.

When an AS, acting as an B2BUA, generates an initial request for a dialog or a or target refresh request, if the contact address it includes in the request possesses the GRUU property (as specified in RFC 5627 [87]) then that contact address should include a 'gruu' URI parameter.

When an AS, acting as a B2BUA, terminates a dialog establishing request or target refresh request, if the contact address it includes in the response possesses the GRUU property (as specified in RFC 5627 [87]) then that contact address should include a 'gruu' URI parameter.

• • •

5.9 IMS-ALG

• • •

The internal function of the IMS-ALG is defined in 3GPP TS 29.162 [11A].

5.10 STUN Server

Stand-alone STUN servers (i.e., STUN servers not associated with a UE or P-CSCF) shall meet the requirements defined by RFC 5389 [83].

5.11 TURN Server

TURN servers shall meet the requirements defined by RFC 5766 [85].

6 Application usage of SDP

6.1 Procedures at the UE

6.1.1 General

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

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect 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.

The UE shall include the "b=" media descriptor and the "TIAS" bandwidth modifier as described in RFC 3890 [90]. The proposed bandwidth for well-known codecs shall be based as defined in the IPCablecom Codec specification [99].

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level different than the default RTCP bandwidth as specified in RFC 4566 [39], then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 [56] to specify the required bandwidth allocation for RTCP.

For other media streams the "b=" media descriptor ~~may~~shall 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 ~~modifer~~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].

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].

In order to support NAT traversal using ICE, RFC 5245 [84], the UE shall advertise candidate addresses as described in section 7.3 of [84]. The format of this attribute is described in section 12 of [84].

The UE shall also support the "a=rtcp" attribute. This requirement is included in RFC 5245 [84] and is defined in RFC 3605 [88].

In order to provide QoS at the access (IPCablecom Multimedia) an appropriate classifier must be provided for the flow traversing the CMTS. The component in the signalling path that makes the IPCablecom Multimedia request (P-CSCF) shall be requested based on the "active" transport address which is the one that is advertised in the "m=" and "c=" lines of the SDP. When a TURN candidate is the active transport address, the value provided is not usable as a classifier for the flow as it traverses the CMTS. The Client shall provide the IP address and port that it sends packets to in an a=Local-TURN attribute of its SDP, when the TURN Address is the active transport Address.

This process requires a new SDP attribute. It is called "Local-TURN". The Local-TURN attribute shall be present within a media block of the SDP. It contains the IP Address and Port the client will send its media to and receive its media from. There shall only be a single Local-TURN attribute in a given media block.

The syntax of this attribute is:

```
Local-TURN                = "TURN" ":" addr SP Port SP
                          ;addr, Port from RFC 2327
```

6.1.2 Handling of SDP at the originating UE

An INVITE request generated by a UE shall contain a SDP offer. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session. The UE shall order the SDP offer with the most preferred codec listed first.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the initial SDP offer, the UE shall:

– indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64], if the UE supports the precondition mechanism (see subclause 5.1.3.1). If the UE requires the use of preconditions, the strength-tag shall be set to "mandatory"; if the UE merely desires to use preconditions, the strength-tag shall be set to "optional", if the UE has no preference on the use of preconditions, the strength-tag shall be set to "none"; and,

NOTE 0 – The "mandatory" strength-tag can only be used when a Require header containing the value "precondition" is included.

– set the related media streams to inactive, by including an "a=inactive" line, according to the procedures described in RFC 4566 [39], only if the precondition mechanism is required and the strength-tag is set to "mandatory".

NOTE 1 – When setting the media streams to the inactive mode, the UE can include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

If the desired QoS resources for one or more media streams are available at the UE when the initial SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type and strength-tag as described above, as defined in RFC 3312 [30] and RFC 4032 [64], if the UE supports the precondition mechanism (see subclause 5.1.3.1).

NOTE 2 – If the originating UE does not support the precondition mechanism it will not include any precondition information in SDP.

~~Upone~~ Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e., a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3 – The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Upon confirming successful local resource reservation, the UE shall create a SDP offer in which the media streams previously set to inactive mode are set to active (sendrecv, sendonly or recvonly) mode.

Upon receiving an SDP answer, which includes more than one codec for one or more media streams, the UE shall send an SDP offer at the first possible time, selecting only one codec per media stream.

6.1.3 Handling of SDP at the terminating UE

Upon receipt of an initial SDP offer in which no precondition information is available, the terminating UE shall in the SDP answer:

– if, prior to sending the SDP answer the desired QoS resources have been reserved at the terminating UE, set the related media streams in the SDP answer to:
  - active mode, if the offered media streams were not listed as inactive; or
  - inactive mode, if the offered media streams were listed as inactive.

If the terminating UE had previously set one or more media streams to inactive mode and the QoS resources for those media streams are now ready, it shall set the media streams to active mode by applying the procedures described in RFC 4566 [39] with respect to setting the direction of media streams.

Upon sending a SDP answer to an SDP offer (which included one or more media lines which was offered with several codecs) the terminating UE shall select exactly one codec per payload and indicate only the selected codec for the related media stream.

NOTE 1 – A SDP media line can indicate several different payloads. For example, a media line indicating an audio media type can indicate several codecs for the audio stream as well as the MIME subtype "telephone-event" for DTMF payload.

Upon sending a SDP answer to an SDP offer, with the SDP answer including one or more media streams for which the originating side indicated its local preconditions as not met, if the precondition mechanism is supported by the terminating UE, the terminating UE shall indicate its local preconditions and request the confirmation for the result of the resource reservation at the originating end point.

NOTE 2 – If the terminating UE does not support the precondition mechanism, it will ignore any precondition information received from the originating UE.

Upon receiving an initial INVITE request, that includes the SDP offer containing an IP address type (in the "c="parameter) that is not supported by the UE, it shall respond with the 488 (Not Acceptable Here) response with 301 Warning header indicating "incompatible network address format".

NOTE 3 – Upon receiving an initial INVITE request, that includes an SDP offer containing connection addresses (in the "c=" parameter) equal to zero, the UE will select the media streams that is willing to accept for the session, reserve the QoS resources for accepted media streams, and include its valid connection address in the SDP answer.~~Upon receipt of an initial SDP offer in which no precondition information is available and the desired QoS resources for one or more media streams have not been reserved at the terminating UE, the UE shall in the SDP answer set the related media streams to inactive mode by including an "a=inactive" line, according to the procedures described in draft-ietf-mmusic-sdp-new [39].~~ ~~If the UE is afterwards setting one or more media streams to active mode, it shall apply the procedures described in draft-ietf-mmusic-sdp-new [39] with respect to setting the direction of media streams.~~

~~Upon sending a SDP answer to an initial SDP offer, with the SDP answer including one or more media streams for which the originating side did indicate its local preconditions as not met, if the~~

~~precondition mechanism is supported by the terminating UE, the terminating UE shall request confirmation for the result of the resource reservation at the originating end point.~~

~~NOTE 1: If the terminating UE does not support the precondition mechanism it will ignore any precondition information received from the originating UE.~~

~~Upon receipt an initial INVITE request, that includes the SDP offer containing an IP address type (in the "c=" parameter) that is not supported by the UE, it shall respond with the 488 (Not Acceptable Here) response with 301 Warning header indicating "incompatible network address format".~~

6.2 Procedures at the P-CSCF

...

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

The UE shall populate the P-Access-Network-Info header, where use is specified in subclause 5.1, 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", ~~or~~ "IEEE-802.11a", ~~or~~ "IEEE-802.11b", ~~or~~ "IEEE-802.11g", or "DOCSIS" as appropriate to the ~~radio~~ access technology in use;

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

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

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

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

4) if the access-type field set to one of "IEEE-802.11", ~~or~~ "IEEE-802.11a", ~~or~~ "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.

7.2A.5 P-Charging-Vector header

...

7.2A.5.2.1 General

The syntax of the P-Charging-Vector header field 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.

Table 7.3 describes 3GPP-specific extensions to the P-Charging-Vector header field defined in RFC 3455 [52].

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

```
access-network-charging-info = (gprs-charging-info / i-wlan-charging-info /
packetcable-charging-info / generic-param)
gprs-charging-info = ggsn SEMI auth-token [SEMI pdp-info-hierarchy] *(SEMI
extension-param)
ggsn = "ggsn" EQUAL gen-value
pdp-info-hierarchy = "pdp-info" EQUAL LDQUOT pdp-info *(COMMA pdp-info) RDQUOT
pdp-info = pdp-item SEMI pdp-sig SEMI gcid [SEMI flow-id]
pdp-item = "pdp-item" EQUAL DIGIT
pdp-sig = "pdp-sig" EQUAL ("yes" / "no")
gcid = "gcid" EQUAL 1*HEXDIG
auth-token = "auth-token" EQUAL 1*HEXDIG
flow-id = "flow-id" EQUAL "(" "{" 1*DIGIT COMMA 1*DIGIT "}" *(COMMA "{" 1*DIGIT
COMMA 1*DIGIT "}")")"
extension-param = token [EQUAL token]
i-wlan-charging-info = "pdg"
packetcable-charging-info = packetcable [SEMI bcid]
packetcable = "packetcable-multimedia"
bcid = "bcid" EQUAL 1*48(HEXDIG)
```

•••

7.2A.5.2.3 I-WLAN as IP-CAN

•••

This version of the specification defines the use of "pdg" for inclusion in the P-Charging-Vector header. No other extensions are defined for use in I-WLAN in this version of the specification.

7.2A.5.2.4 IPCablecom as IP-CAN

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of the P-Charging-Vector header. The access-network-charging-info parameter includes alternative definitions for different types of access networks. This subclause defines the components of the cable instance of the access-network-charging-info.

For IPCablecom there is the following component to track: the billing correlation identifier (bcid) that uniquely identifies the IPCablecom bearer resources associated with the session within the operator's network for the purposes of billing correlation. To facilitate the correlation of session and bearer accounting events, a correlation ID that uniquely identifies the resources associated with a session is needed. This is accomplished through the use of the bcid as generated by the IPCablecom Multimedia network. This bcid is returned to the P-CSCF within the response to a successful resource request.

The bcid is specified in RFC 3603 [92] as a 24-byte binary structure, containing 4 bytes of NTP timestamp, 8 bytes of the unique identifier of the network element that generated the ID, 8 bytes giving the time zone, and 4 bytes of monotonically increasing sequence number at that network element. This identifier is chosen to be globally unique within the system for a window of several months. This must be encoded as a hexadecimal string of up to 48 characters. Leading zeroes may be suppressed.

If the bcid value is received in binary format at the P-CSCF, the P-CSCF shall encode it in hexadecimal format before including it into the bcid parameter. On receipt of this header, a node receiving a bcid shall decode from hexadecimal into binary format.

If there is no authorization activity or information exchange with the IPCablecom Multimedia network, the bcid parameter shall be omitted from the access-network-charging-info parameter.

7.2A.5.3 Operation

…

7.7 SIP timers

The timers defined in RFC 3261 [26] need modification in some cases to accommodate the delays introduced by the air interface processing and transmission delays. Table 7.8 shows recommended values for IM CN subsystem.

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

The second column, titled "value to be applied between IM CN subsystem elements" lists the values recommended for network elements e.g., P-CSCF, S-CSCF, MGCF, when communicating with each other i.e., when no air interface leg is included. These values are identical to those recommended by RFC 3261 [26].

The third column, titled "value to be applied at the UE" lists the values recommended for the UE, when in normal operation the UE generates requests or responses containing a P-Access-Network-Info header which included a value of "3GPP-GERAN", "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", or "IEEE-802.11g". These are modified when compared to RFC 3261 [26] to accommodate the air interface delays. In all other cases, the UE should use the values specified in RFC 3261 [26] as indicated in the second column of Table 7.8.

The fourth column, titled "value to be applied at the P-CSCF toward a UE" lists the values recommended for the P-CSCF when an air interface leg is traversed, and which are used on all SIP transactions on a specific security association where the security association was established using a REGISTER request containing a P-Access-Network-Info header which included a value of "3GPP-GERAN", "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "IEEE-802.11", "IEEE-802.11a" or "IEEE-802.11b", or "IEEE-802.11g". These are modified when compared to RFC 3261 [26]. In all other cases, the P-CSCF should use the values specified in RFC 3261 [26] as indicated in the second column of Table 7.8.

When the UE is unaware of the access technology and is unable to provide a P-Access-Network-Info header, both the UE and the P-CSCF should use the values specified in RFC 3261 [26] as indicated in the second column of Table 7.8. This ensures consistent application of the SIP timer values between the UE and P-CSCF.

Editor's note – For WLAN, it is FFS if it is considered as a radio access or a broadband access for the recommended timer values.

Editor's note – Further study is needed as to whether there are better means of determining the access technology delays between the P-CSCF and a UE, and therefore the conditions under which the extended values of the timers should apply.

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

Table 7.8 – SIP timers

SIP Timer	Value to be applied between IM CN subsystem elements	Value to be applied at the UE	Value to be applied at the P-CSCF toward a UE	Meaning
T1	500ms default	2s default	2s default	RTT estimate
T2	4s	16s	16s	The maximum retransmit interval for non-INVITE requests and INVITE responses
T4	5s	17s	17s	Maximum duration a message will remain in the network
Timer A	initially T1	initially T1	initially T1	INVITE request retransmit interval, for UDP only
Timer B	64*T1	64*T1	64*T1	INVITE transaction timeout timer
Timer C	> 3min	> 3 min	> 3 min	proxy INVITE transaction timeout
Timer D	> 32s for UDP	>128s	>128s	Wait time for response retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
Timer E	initially T1	initially T1	initially T1	non-INVITE request retransmit interval, UDP only
Timer F	64*T1	64*T1	64*T1	non-INVITE transaction timeout timer
Timer G	initially T1	initially T1	initially T1	INVITE response retransmit interval
Timer H	64*T1	64*T1	64*T1	Wait time for ACK receipt.
Timer I	T4 for UDP	T4 for UDP	T4 for UDP	Wait time for ACK retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
Timer J	64*T1 for UDP	64*T1 for UDP	64*T1 for UDP	Wait time for non-INVITE request retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	
Timer K	T4 for UDP	T4 for UDP	T4 for UDP	Wait time for response retransmits
	0s for TCP/SCTP	0s for TCP/SCTP	0s for TCP/SCTP	

7.8 IM CN subsystem timers

…

8 SIP compression

8.1 SIP compression procedures at the UE

8.1.1 SIP compression

If in normal operation the UE generates requests or responses containing a P-Access-Network-Info header which included a value of "3GPP-GERAN", "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", or

"IEEE-802.11g", then the~~The~~ UE shall support SigComp as specified in RFC 3320 [32]. When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486 [55]. When the UE will create the compartment is implementation specific, but the compartment shall not be created until a set of security associations are set up. The compartment shall finish when the UE is deregistered. State creations and announcements shall be allowed only for messages received in a security association.

Editor's note – For WLAN, it is FFS if it is considered as a radio access or a broadband access for the recommended use of compression.

NOTE – Exchange of bytecodes during registration will prevent unnecessary delays during session setup.

~~Editor's note: The draft-ietf-rohc-sigcomp-sip-01 [79] can lead to the need for additional changes or clarifications.~~

If the UE supports SigComp (as described in RFC 5049 [79]), then the~~The~~ UE shall support the SIP dictionary specified in RFC 3485 [42]. If compression is enabled, the UE shall use the dictionary to compress the first message.

The following apply when signalling compression is used:

- State Memory Size greater than zero is needed to give room for the UDVM byte code and make dynamic compression possible. A State Memory Size of at least 4096 bytes shall be a minimum value; and
- A Decompression Memory Size of at least 8192 bytes shall be a minimum value.

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

If in normal operation the UE generates requests or responses containing a P-Access-Network-Info header which included a value of "3GPP-GERAN", "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b", or IEEE-802.11g", then the~~The~~ UE should compress the requests and responses transmitted to the P-CSCF according to subclause 8.1.1. In other cases where SigComp is supported, it need not.

Editor's NOTE – For WLAN, it is FFS if it is considered as a radio access or a broadband access for the recommended use of compression.

NOTE 1 – Compression of SIP messages is an implementation option. However, compression is strongly recommended.

NOTE 2 – In an IP-CAN where~~Since~~ compression support is mandatory, the UE may send even the first message compressed. Sigcomp provides mechanisms to allow the UE to know if state has been created in the P-CSCF or not.

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

If the UE supports SigComp, then the ~~The~~UE shall decompress the compressed requests and responses received from the P-CSCF according to subclause 8.1.1.

If the UE detects a decompression failure at the P-CSCF, the recovery mechanism is implementation specific.

• • •

8.2.2 Compression of SIP requests and responses transmitted to the UE

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

Editor's note – Further study is needed as to whether there are better means of determining the access technology delays between the P-CSCF and a UE, and therefore the conditions under which compression should apply.

For all SIP transactions on a specific security association where the security association was established using a REGISTER request containing a P-Access-Network-Info header which included a value of "3GPP-GERAN", "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD", "3GPP2-1X", "3GPP2-1X-HRPD", "IEEE-802.11", "IEEE-802.11a", "IEEE-802.11b" or "IEEE-802.11g" then the P-CSCF should compress the requests and responses transmitted to the UE according to subclause 8.2.1. In other cases where SigComp is supported, it need not.

Editor's note – For WLAN, it is FFS if it is considered as a radio access or a broadband access for the recommended use of compression

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

• • •

9.2.1 Connecting to the IP-CAN and P-CSCF discovery

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

a) establish a connection with the IP-CAN;

b) obtain an IP address using either the standard IETF protocols (e.g., DHCP or IPCP) or a protocol that is particular to the IP-CAN technology that the UE is utilising. The obtained IP address shall be fixed throughout the period the UE is connected to the IM CN subsystem, i.e., from the initial registration and at least until the last deregistration; and

c) acquire a P-CSCF address(es).

The methods for acquiring a P-CSCF address(es) are:

I. Employ Dynamic Host Configuration Protocol for IPv4 RFC 2131 [40A] or for IPv6 (DHCPv6) RFC 3315 [40] and the DHCP~~v6~~ options for SIP servers RFC 3319 [41] in case of IPv6 and RFC 3361 [103] in case of IPv4).

The UE shall either:

- in the DHCP query, request a list of SIP server domain names of P-CSCF(s) and the list of Domain Name Servers (DNS); or
- request a list of SIP server IP~~v6~~ addresses of P-CSCF(s).

II. Obtain the P-CSCF address(es) by employing a procedure that the IP-CAN technology supports. (e.g., GPRS).

When acquiring a P-CSCF address(es) the UE can freely select either method I or II.

The UE may also request a DNS Server IP~~v6~~ address(es) as specified in RFC 3315 [40] or RFC 2131 [40A].

9.2.2 Handling of the IP-CAN

• • •

Annex A (normative)

Profiles of IETF RFCs for 3GPP usage

• • •

A.1.3 Roles

• • •

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
41	DOCSIS	[52] 4.4	o	c1

c1: If A.3/1 OR A.3/2 THEN o.1 ELSE n/a.

o: It is mandatory to support at least one of these items.

A.2 Profile definition for the Session Initiation Protocol as used in the present document

• • •

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	c19~~8~~
15	the REFER method?	[36]	o	c33
16	integration of resource management and SIP?	[30] [64]	c19	c19~~8~~
17	the SIP UPDATE method?	[29]	c5	c5~~18~~
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

Table A.4 – Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
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
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
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
40D	the recurse-directive within caller-preferences?	[56B] 9.1	o.5	o.5

Table A.4 – Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
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 ~~Inititation~~Initiation Protocol (SIP) "Replaces" header?	[60]	c19	c19 (note 1)
45	the Session ~~Inititation~~Initiation Protocol (SIP) "Join" header?	[61]	c19	c19 (note 1)
46	the callee capabilities?	[62]	o	c35
47	Managing Client Initiated Connections?	[86]	o	c43

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 m ELSE n/a – UE behaviour.~~ 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 THEN m ELSE IF A.3/2 THEN o ELSE n/a – UE or P-CSCF.

c15: IF A.4/20 AND (A.3/4 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)~~ A.3/1 THEN o ELSE 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 or UA.

Table A.4 – Major capabilities

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 ~~Inititation~~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 ~~Inititation~~Initiation Protocol (SIP) "Replaces" header or the Session ~~Inititation~~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.

c43: IF A.3/1 OR A.3/4 THEN m ELSE n/a – UE or S-CSCF.

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.

Editor's note: For WLAN, it is FFS if it is considered as a radio access or a broadband access for the recommended use of compression.

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

Table A.4A – Supported event packages

Item	Does the implementation support	Subscriber			Notifier		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
5	presence.winfo template-package?	[72] 4	c1	c9	[72] 4	c2	c10
6	sip-profile package?	~~[77]~~ Clause E.3	c1	c11	~~[77]~~ Clause E.3	c2	c12
7	conference package?	[78] 3	c1	c21	[78] 3	c1	c22

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.3/1 OR A.3/7) THEN o ELSE n/a – ~~UE,~~ P-CSCF, UE, 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.

…

A.2.1.4.12 REGISTER method

…

Table A.123 – Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
1A	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	m	m
1B	Accept-Language	[26] 20.3	o	o	[26] 20.3	m	m
2	Allow-Events	[28] 7.2.2	c12	c12	[28] 7.2.2	c13	c13
3	Authentication-Info	[26] 20.6	c6	c6	[26] 20.6	c7	c7
5	Contact	[26] 20.10	o	o	[26] 20.10	m	m
5A	P-Associated-URI	[52] 4.1	c8	c9	[52] 4.1	c10	c11
6	Path	[35] 4	c3	c3	[35] 4	c4	c4
8	Service-Route	[38] 5	c5	c5	[38] 5	c5	c5
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m

c1: IF (A.3/4 AND A.4/2) THEN m ELSE n/a. – S-CSCF acting as registrar.

c2: IF A.3/4 OR A.3/1THEN m ELSE n/a. – S-CSCF or UE.

c3: IF A.4/24 THEN m ELSE n/a – session initiation protocol extension header field for registering non-adjacent contacts.

c4: IF A.4/24 THEN o ELSE n/a – session initiation protocol extension header field for registering non-adjacent contacts.

c5: IF A.4/28 THEN m ELSE n/a – session initiation protocol extension header field for service route discovery during registration.

c6: IF A.4/8 THEN o ELSE n/a – authentication between UA and registrar.

c7: IF A.4/8 THEN m ELSE n/a – authentication between UA and registrar.

c8: IF A.4/2 AND A.4/31 THEN m ELSE n/a – P-~~Assocated~~Associated-URI header extension and registrar.

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

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

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

c12: IF A.4/20 THEN o ELSE n/a – SIP specific event notification extension.

c13: IF A.4/20 THEN m ELSE n/a – SIP specific event notification extension.

• • •

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

Table A.162 – Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
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

Table A.162 – Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
31E	application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs?	[33] 5.2	n/a	n/a
31F	application of the privacy option "user" such that user level privacy functions are provided by the network?	[33] 5.3	n/a	n/a
31G	application of the privacy option "id" such that privacy of the network asserted identity is provided by the network?	[34] 7	c11	c12
32	Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration	[38]	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

Table A.162 – Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
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 ~~Inititation~~Initiation Protocol (SIP) "Replaces" header?	[60]	o	o
55	the Session ~~Inititation~~Initiation Protocol (SIP) "Join" header?	[61]	o	o
56	the callee ~~capabillities~~ capabilities?	[62]	o	o
57	Managing Client Initiated Connections?	[864]	o	c34

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.

Table A.162 – Major capabilities

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 o – P-CSCF or S-CSCF of MGCF.

c30: IF A.3/2 o ELSE i o – P-CSCF.

c31: IF A.3/4 THEN m ELSE x o – S-CSCF.

c32: IF A.3/4 THEN m ELSE o.4 o – 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 o – support of any directives within caller preferences for the session initiation protocol.

c34: IF A.3/2 OR A.3/4 THEN m ELSE n/a o – P-CSCF or S-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.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)
26	Interactive Connectivity Establishment (ICE)	[84]	o	c2
26A	Gathering Candidate Addresses	[84]	o	c3
26B	Connectivity Checks	[84]	o	c1

c1: IF A.3/1 THEN m ELSE n/a – UE role.

c2: IF A.317/26A OR A.317/26B THEN m ELSE n/a

c3: IF A.3/1 and UE can be deployed behind a NAT THEN m ELSE n/a – UE role.

NOTE 1 – For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified.

A.3.2.2 SDP types

Table A.318 – SDP types

Item	Type	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
	Session level description						
1	v= (protocol version)	[39] 6	m	m	[39] 6	m	m
2	o= (owner/creator and session identifier)	[39] 6	m	m	[39] 6	m	m
3	s= (session name)	[39] 6	m	m	[39] 6	m	m
4	i= (session information)	[39] 6	o	o	[39] 6	m	m
5	u= (URI of description)	[39] 6	o	n/a	[39] 6	o	n/a
6	e= (email address)	[39] 6	o	n/a	[39] 6	o	n/a
7	p= (phone number)	[39] 6	o	n/a	[39] 6	o	n/a
8	c= (connection information)	[39] 6	o	o	[39] 6	m	m
9	b= (bandwidth information)	[39] 6	o	o (Note 1)	[39] 6	m	m
	Time description (one or more per description)						
10	t= (time the session is active)	[39] 6	m	m	[39] 6	m	m

Table A.318 – SDP types

Item	Type	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
11	r= (zero or more repeat times)	[39] 6	o	n/a	[39] 6	o	n/a
	Session level description (continued)						
12	z= (time zone adjustments)	[39] 6	o	n/a	[39] 6	o	n/a
13	k= (encryption key)	[39] 6	o	o	[39] 6	o	o
14	a= (zero or more session attribute lines)	[39] 6	o	o	[39] 6	m	m
	Media description (zero or more per description)						
15	m= (media name and transport address)	[39] 6	o	o	[39] 6	m	m
16	i= (media title)	[39] 6	o	o	[39] 6	o	o
17	c= (connection information)	[39] 6	c1	c1	[39] 6	c1	c1
18	b= (bandwidth information)	[39] 6	o	o (Note 1)	[39] 6		
19	k= (encryption key)	[39] 6	o	o	[39] 6	o	o
20	a= (zero or more media attribute lines)	[39] 6	o	o	[39] 6	m	m

c1: IF A.318/15 THEN m ELSE n/a.
NOTE 1 – For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified. IPCablecom implementation shall use the b=TIAS as described in [90].

Prerequisite A.318/14 OR A.318/20 – a= (zero or more session/media attribute lines)

Table A.319 – Zero or more session / media attribute lines (a=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	category (a=cat)	[39] 6			[39] 6		
2	keywords (a=keywds)	[39] 6			[39] 6		
3	name and version of tool (a=tool)	[39] 6			[39] 6		
4	packet time (a=ptime)	[39] 6	o	M (Note 1)	[39] 6		
5	maximum packet time (a=maxptime)	[39] 6			[39] 6		
6	receive-only mode (a=recvonly)	[39] 6			[39] 6		
7	send and receive mode (a=sendrecv)	[39] 6			[39] 6		

Table A.319 – Zero or more session / media attribute lines (a=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
8	send-only mode (a=sendonly)	[39] 6			[39] 6		
9	whiteboard orientation (a=orient)	[39] 6			[39] 6		
10	conference type (a=type)	[39] 6			[39] 6		
11	character set (a=charset)	[39] 6			[39] 6		
12	language tag (a=sdplang)	[39] 6			[39] 6		
13	language tag (a=lang)	[39] 6			[39] 6		
14	frame rate (a=framerate)	[39] 6			[39] 6		
15	quality (a=quality)	[39] 6			[39] 6		
16	format specific parameters (a=fmtp)	[39] 6			[39] 6		
17	rtpmap attribute (a=rtpmap)	[39] 6			[39] 6		
18	current-status attribute (a=curr)	[30] 5	c1	c1	[30] 5	c2	c2
19	desired-status attribute (a=des)	[30] 5	c1	c1	[30] 5	c2	c2
20	confirm-status attribute (a=conf)	[30] 5	c1	c1	[30] 5	c2	c2
21	media stream identification attribute (a=mid)	[53] 3	c3	c3	[53] 3	c4	c4
22	group attribute (a=group)	[53] 4	c5	c5	[53] 3	c6	c6
23	candidate IP addresses (a=candidate) Maximum packet rate (a=maxprate)	[84] [80]	c7o	c7o (Note 2)	[84]	c8	c8

c1: IF A.317/22 THEN o ELSE n/a.
c2: IF A.317/22 THEN m ELSE n/a.
c3: IF A.317/23 THEN o ELSE n/a.
c4: IF A.317/23 THEN m ELSE n/a.
c5: IF A.317/24 THEN o ELSE n/a.
c6: IF A.317/24 THEN m ELSE n/a.
c7: IF A.317/26 THEN o ELSE n/a.
c8: IF A.317/26 THEN m ELSE n/a.

NOTE 1 – The UE must include the ptime and it MUST be used to indicate the packetization time with which the UE expects to receive traffic.

NOTE 2 – For well-known codecs this is optional. For non-well-known codecs, it shall be specified as per [90] (i.e., a=maxprate).

• • •

[Editor's note: The following Annex E has been added, but it is not shown with revision marks.]

Annex E[1]

A framework for Session Initiation Protocol user agent profile delivery

E.1 Introduction

SIP User Agents require configuration data to function properly. Examples include local network, device and user specific information. A configuration data set specific to an entity is termed a profile. For example, device profile contains the configuration data related to a device. The process of providing devices with one or more profiles is termed profile delivery. Ideally, this profile delivery process should be automatic and require minimal or no user intervention.

Many deployments of SIP User Agents require dynamic configuration and cannot rely on pre-configuration. This framework provides a standard means of providing dynamic configuration which simplifies deployments containing SIP User Agents from multiple vendors. This framework also addresses change notifications when profiles change. However, the framework does not define the content or format of the profile, leaving that to future standardization activities.

This annex is organized as follows. Clause E.3 provides a high-level overview of the abstract components, profiles, and the profile delivery stages. Clause E.4 provides some motivating use cases. Clause E.5 provides details of the framework operation and requirements. Clause E.6 provides a concise event package definition. Clause E.7 follows with illustrative examples of the framework in use.

E.2 Terminology and conventions used within this annex

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this annex are to be interpreted as described in RFC 2119 [100].

This annex also reuses the SIP terminology defined in RFC 3261 [26] and RFC 3265 [28], and specifies the usage of the following terms.

device: Software or hardware entity containing one or more SIP user agents. It may also contain entities such as a DHCP client.

device provider: The entity responsible for managing a given device.

local network provider: The entity that controls the local network to which a given device is connected.

SIP service provider: The entity providing SIP services to users. This can refer to private enterprises or public entities.

profile: Configuration data set specific to an entity (e.g., user, device, local network or other).

profile type: A particular category of Profile data (e.g., User, Device, Local Network or other).

profile delivery server (PDS): The source of a Profile, it is the logical collection of the Profile Notification Component (PNC) and the Profile Content Component (PCC).

[1] This annex is based upon draft-ietf-sipping-config-framework-17 and is included with the kind permission of its authors, Dan Petrie and Sumanth Channabasappa.

profile notification component (PNC): The logical component of a Profile Delivery Server that is responsible for enrolling devices and providing profile notifications.

profile content component (PCC): The logical component of a Profile Delivery Server that is responsible for storing, providing access to, and accepting profile content.

profile delivery stages: The processes that lead a device to obtain profile data, and any subsequent changes, are collectively called profile delivery stages.

bootstrapping: Bootstrapping is the process by which a new (or factory reset) device, with no configuration or minimal "factory" pre-configuration, enrols with the PDS. The device may use a temporary identity and credentials to authenticate itself to enrol and receive profiles, which may provide more permanent identities and credentials for future enrolments.

E.3 Overview

This clause provides an overview of the configuration framework. It presents the reference model, the motivation, the profile delivery stages and a mapping of the concepts to specific use cases. It is meant to serve as a reference clause for the document, rather than providing a specific logical flow of material, and it may be necessary to revisit these sections for a complete appreciation of the framework.

The SIP UA Profile Delivery Framework uses a combination of SIP event messages (SUBSCRIBE and NOTIFY; RFC 3265 [28]) and traditional file retrieval protocols, such as HTTP [101], to discover, monitor, and retrieve configuration profiles. The framework defines three types of profiles (local-network, device, and user) in order to separate aspects of the configuration which may be independently managed by different administrative domains. The initial SUBSCRIBE message for each profile allows the UA to describe itself (both its implementation and the identity requesting the profile), while requesting access to a profile by type, without prior knowledge of the profile name or location. Discovery mechanisms are specified to help the UA form the subscription URI (the Request-URI for the SIP SUBSCRIBE). The SIP UAS handling these subscriptions is the Profile Delivery Server (PDS). When the PDS accepts a subscription, it sends a NOTIFY to the device. The initial NOTIFY from the PDS for each profile may contain profile data or a reference to the location of the profile, to be retrieved using HTTP or similar file retrieval protocols. By maintaining a subscription to each profile, the UA will receive additional NOTIFY messages if the profile is later changed. These may contain a new profile, a reference to a new profile, or a description of profile changes, depending on the Content-Type RFC 3261 [26] in use by the subscription. The framework describes the mechanisms for obtaining three different profile types, but does not describe the data model they utilize (the data model is out of scope for this specification).

E.3.1 Reference Model

The design of the framework was the result of a careful analysis to identify the configuration needs of a wide range of SIP deployments. As such, the reference model provides for a great deal of flexibility, while breaking down the interactions to their basic forms, which can be reused in many different scenarios.

The reference model for the framework defines the interactions between the Profile Delivery Server (PDS) and the device. The device needs the profile data to function effectively in the network. The PDS is responsible for responding to device requests and providing the profile data. The reference model is illustrated in Figure E.1.

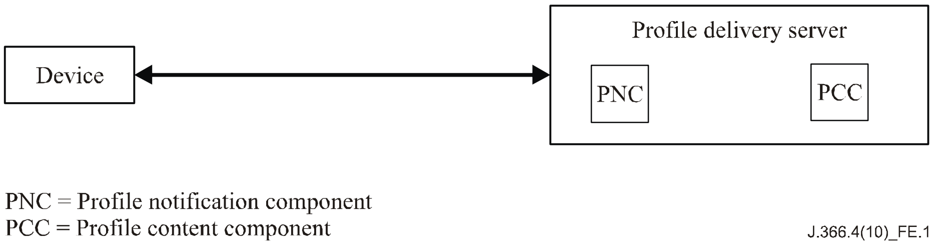
Device
Profile delivery server
PNC
PCC
PNC = Profile notification component
PCC = Profile content component
J.366.4(10)_FE.1

Figure E.1 – Framework Reference Model

The PDS is subdivided into two logical components:

- Profile Notification Component (PNC), responsible for enrolling devices for profiles and providing profile change notifications;
- Profile Content Component (PCC), responsible for storing, providing access to, and accepting modifications related to profile content.

E.3.2 Motivation

The motivation for the framework can be demonstrated by applying the reference model presented in clause E.3.1 to two scenarios that are representative of the two ends of a spectrum of potential SIP deployments.

In the simplest deployment scenario, a device connects through a network that is controlled by a single provider who provides the local-network, manages the devices, and offers services to the users. The provider propagates profile data to the device that contains all the necessary information to obtain services in the network (including information related to the local-network and the users). This is illustrated in Figure E.2. An example is a simple enterprise network that supports SIP-based devices.

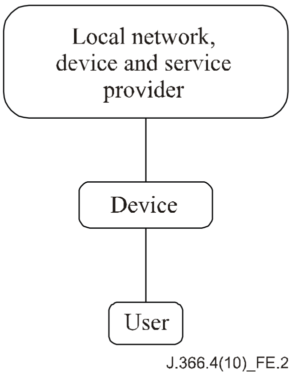

Figure E.2 – Simple Deployment Model

In more complex deployments, devices connect via a local network that is not controlled by the SIP Service Provider, such as devices that connect via available public WiFi hot spots. In such cases, local network providers may wish to provide local network information such as bandwidth constraints to the devices.

Devices may also be controlled by device providers that are independent of the SIP service provider who provides user services, such as kiosks that allow users to access services from remote locations. In such cases the profile data may have to be obtained from different profile sources: local network provider, device provider and SIP service provider. This is indicated in Figure E.3.

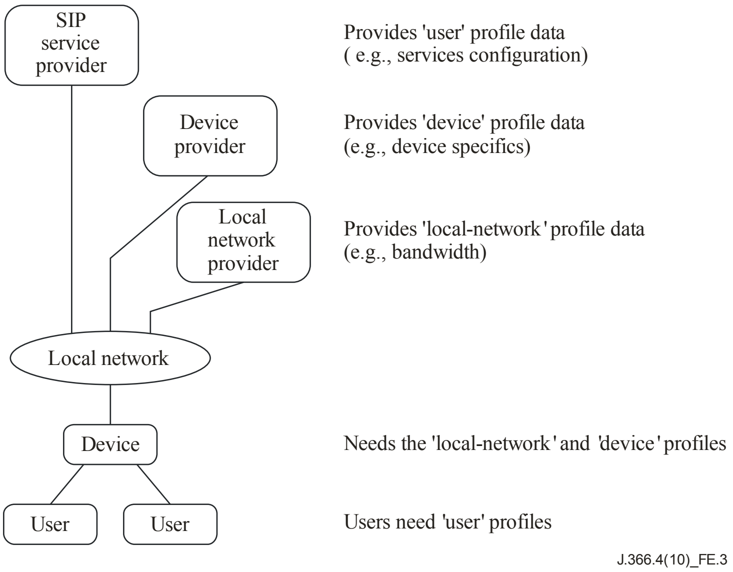
SIP service provider
Provides 'user' profile data (e.g., services configuration)
Device provider
Provides 'device' profile data (e.g., device specifics)
Local network provider
Provides 'local-network' profile data (e.g., bandwidth)
Local network
Device
Needs the 'local-network' and 'device' profiles
User
User
Users need 'user' profiles
J.366.4(10)_FE.3

Figure E.3 – Complex Deployment Model

In either case, Providers need to deliver to the device, profile data that is required to participate in their network. Examples of profile data include the list of codecs that can be used and the SIP proxies to connect to for services. Pre-configuration of such information is one option if the device is always served by the same set of Providers. In all other cases, the profile delivery needs to be automated and consistent across Providers. Given the presence of a number of large deployments where pre-configuration is neither desired nor optimal, there is a need for a common configuration framework such as the one described in this document.

Further, the former deployment model can be accomplished by the device obtaining profile data from a single provider. However, the latter deployment model requires the device to obtain profile data from different providers. To address either deployment, or any variation in between, one needs to allow for profile delivery via one, or more, Providers. The framework accomplishes this by specifying multiple profile types and a set of profile delivery stages to obtain them. These are introduced in the clauses to follow.

E.3.3 Profile Types

The framework handles the presence of potentially different Providers by allowing for multiple profile types. Clients request each profile separately, and obtain them from the same, or different, Providers. A deployment can also choose to pre-configure the device to request only a subset of the specified profile types. The framework specifies three basic profile types, as follows:

- **Local Network Profile**: contains configuration data related to the local network to which a device is directly connected, provided by the Local Network Provider.
- **Device Profile**: contains configuration data related to a specific device, provided by the Device Provider.
- **User Profile**: contains configuration data related to a specific User, as required to reflect that user's preferences and the particular services subscribed to. It is provided by the SIP Service Provider.

Additional profile types may also be specified.

PDSs and devices will implement all the three profile types. A device that has not been configured otherwise will try to obtain all the three profile types, in the order specified by this framework. A device being bootstrapped SHOULD request the device profile type (see clause E.5.3.1 for more information). The device can be configured with a different behaviour via profile data previously obtained by the device, or by using other means such as pre-configuration or manual configuration. The data models associated with each profile type are out of scope for this document. Follow-on standardization activities are expected to specify such data models.

E.3.4 Profile delivery stages

The framework specified in this document requires a device to explicitly request profiles. It also requires one or more PDSs which provide the profile data. The processes that lead a device to obtain profile data, and any subsequent changes, can be explained in three stages, termed the profile delivery stages.

- **Profile Enrolment**: the process by which a device requests, and if successful, enrols with a PDS capable of providing a profile. A successful enrolment is indicated by a notification containing the profile information (contents or content indirection information). Depending on the request, this could also result in a subscription to notification of profile changes.
- **Profile Content Retrieval**: the process by which a device retrieves profile contents, if the profile enrolment resulted in content indirection information.
- **Profile Change Notification**: the process by which a device is notified of any changes to an enrolled profile. This may provide the device with modified profile data or content indirection information.

E.4 Use cases

This clause provides a small, non-comprehensive set of representative use cases to further illustrate how this Framework can be utilized in SIP deployments. The first use case is simplistic in nature, whereas the second is relatively complex. The use cases illustrate the effectiveness of the framework in either scenario.

For Security Considerations please refer to clauses E.5 and E.9.

E.4.1 Simple Deployment Scenario

Description: Consider a deployment scenario (e.g., a small private enterprise) where a participating device implements this framework and is configured, using previously obtained profile data, to request only the device profile. Assume that the device operates in the same network as the PDS (i.e., there is no NAT) and it obtains its IP configuration using DHCP. Typical communication between the device and the PDS will traverse one or more SIP proxies, but is not required, and is omitted in this illustration.

Figure E.4 illustrates the sequence of events that include device startup and a successful profile enrolment for the device profile that results in device profile data. It then illustrates how a change in the profile data is delivered via a Profile Change Notification.

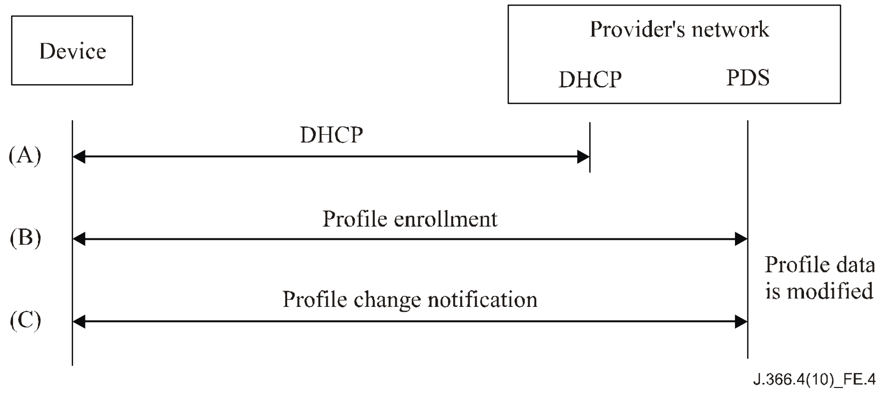

Figure E.4 – Use case 1

The following is an explanation of the interactions in Figure E.4.

(A) Upon initialization, the device obtains IP configuration parameters such as IP address using DHCP.

(B) The device requests profile enrolment for the device profile. Successful enrolment provides it with a notification containing the device profile data.

(C) Due to a modification of the device profile, a profile change notification is sent across to the device, along with the modified profile.

E.4.2 Devices supporting multiple users from different service providers

Description: Consider a single device that allows multiple users to obtain services from different SIP Service Providers, e.g., a kiosk at an airport.

The following assumptions apply:

- Provider A is the Device and Local Network Provider for the device, and the SIP Service Provider for user A; Provider B is the SIP Service Provider for user B.
- Profile enrolment always results in content indirection information requiring profile content retrieval.
- Communication between the device and the PDSs is facilitated via one or more SIP proxies (only one is shown in the illustration).

Figure E.5 illustrates the use case and highlights the communications relevant to the framework specified in this document.

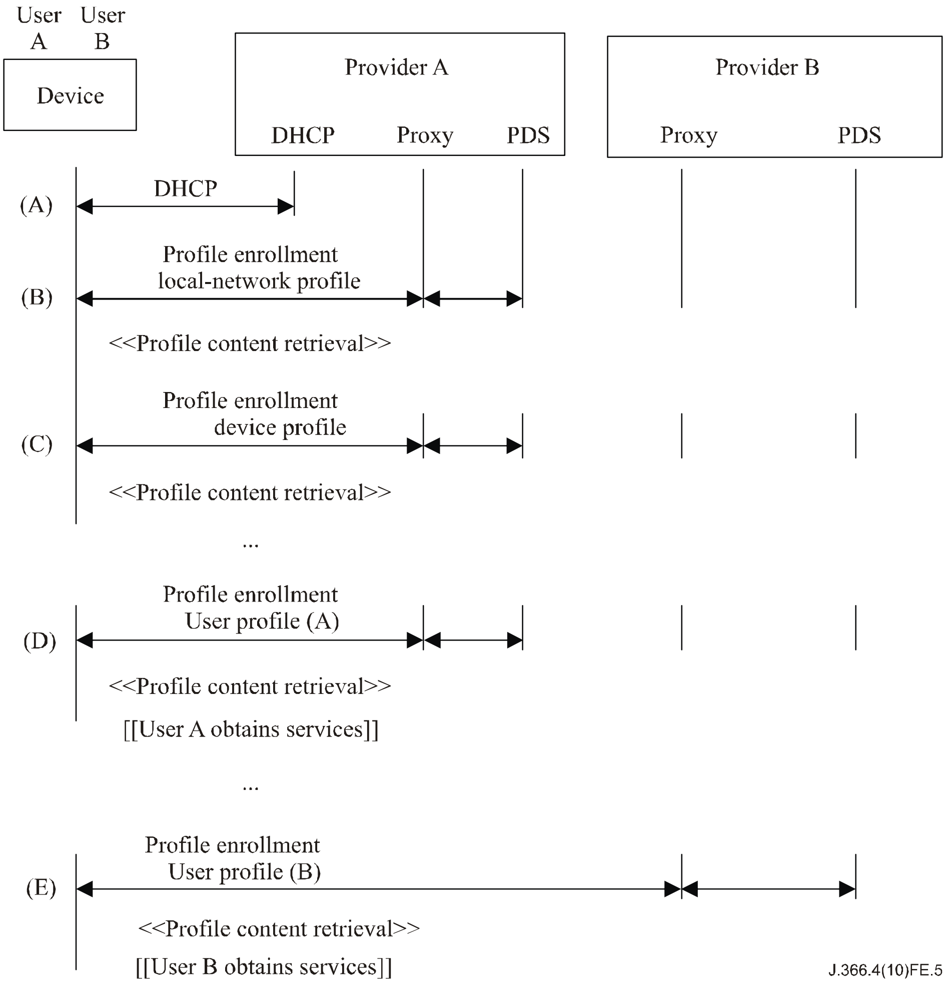
User A
User B
Device
Provider A
DHCP
Proxy
PDS
Provider B
Proxy
PDS
(A)
DHCP
(B)
Profile enrollment local-network profile
<<Profile content retrieval>>
(C)
Profile enrollment device profile
<<Profile content retrieval>>
...
(D)
Profile enrollment User profile (A)
<<Profile content retrieval>>
[[User A obtains services]]
...
(E)
Profile enrollment User profile (B)
<<Profile content retrieval>>
[[User B obtains services]]
J.366.4(10)FE.5

Figure E.5 – Use case 2

The following is an explanation of the interactions in Figure E.5.

(A) Upon initialization, the device obtains IP configuration parameters using DHCP. This also provides the local domain information to help with local-network profile enrolment.

(B) The device requests profile enrolment for the local network profile. It receives an enrolment notification containing content indirection information from Provider A's PDS. The device retrieves the profile (this contains useful information such as firewall port restrictions and available bandwidth).

(C) The device then requests profile enrolment for the device profile. It receives an enrolment notification resulting in device profile content retrieval. The device initializes the user interface for services.

(D) User A with a pre-existing service relationship with Provider A attempts communication via the user Interface. The device uses the user supplied information (including any credential information) and requests profile enrolment for user A's profile. Successful enrolment and profile content retrieval results in services for user A.

(E) At a different point in time, user B with a service relationship with Provider B attempts communication via the user Interface. It enrols and retrieves user B's profile and this results in services for user B.

The discovery mechanisms for profile enrolment described by the framework, or the profile data themselves, can result in outbound proxies that support devices behind NATs, using procedures specified in [86].

E.5 Profile delivery framework

This clause specifies the profile delivery framework. It provides the requirements for the three profile delivery stages introduced in clause E.3.4 and presents the associated security requirements. It also presents considerations such as back-off and retry mechanisms.

E.5.1 Profile delivery stages

The three profile delivery stages – enrolment, content retrieval and change notification – apply separately to each profile type specified for use with this framework. The following clauses provide the requirements associated with each stage.

E.5.1.1 Profile enrolment

Profile enrolment is the process by means of which a device requests, and receives, profile data. Each profile type specified in this document requires an independent enrolment request. However, a particular PDS can support enrolment for one or more profile types.

Profile enrolment consists of the following operations, in the specified order.

1 Enrolment request transmission

Profile enrolment is initiated when the device transmits a SIP SUBSCRIBE request RFC 3265 [28] for the 'ua-profile' event package, specified in clause E.6. The profile being requested is indicated using the 'profile-type' parameter. The device MUST transmit the SIP SUBSCRIBE message via configured outbound proxies for the destination domain, or in accordance with RFC 3263 [27A].

The device needs certain data to create an enrolment request, form a Request-URI, and authenticate to the network. This includes the profile provider's domain name, identities and credentials. Such data can be "configured" during device manufacturing, by the user, or via profile data enrolment (see clause E.5.3.1). The data can also be "discovered" using the procedures specified by this framework. The "discovered" data can be retained across device resets (but not across factory resets) and such data is referred to as "cached". Thus, data can be configured, discovered or cached. The following requirements apply.

- If the device is configured with a specific domain name (for the local network provider or device provider), it MUST NOT attempt "discovery" of the domain name. This is the case when the device is pre-configured (e.g., via a user interface) to be managed by specific entities.
- The device MUST only use data associated with the provider's domain in an enrolment request. As an example, when the device is requesting a local-network profile in the domain 'example.net', it cannot present a user AoR associated with the local domain 'example.com'.
- The device SHOULD adhere to the following order of data usage: configured, cached and discovered. An exception is when the device is explicitly configured to use a different order.

Upon failure to obtain the profile using any methods specified in this framework, the device MAY provide a user interface to allow for user intervention. This can result in temporary, one-time data to bootstrap the device. Such temporary data is not considered to be "configured" and SHOULD NOT be cached across resets. The configuration obtained using such data MAY provide the configuration data required for the device to continue functioning normally.

Devices attempting enrolment MUST comply with the SIP-specific event notification specified in RFC 3265 [28], the event package requirements specified in clause E.6.2, and the security requirements specified in clause E.5.2.

2 Enrolment request admittance

A PDS or a SIP proxy will receive a transmitted enrolment request. If a SIP infrastructure element receives the request, it will relay it to the authoritative proxy for the domain indicated in the Request-URI (the same way it would handle any other SUBSCRIBE message). The authoritative proxy is required to examine the request (e.g., event package) and transmit it to a PDS capable of addressing the profile enrolment request.

A PDS receiving the enrolment request SHOULD respond to the request, or proxy it to a PDS that can respond. An exception to responding or proxying the request is when a policy prevents response (e.g., recognition of a DoS attack, an invalid device, etc.). The PDS then verifies the identity presented in the request and performs any necessary authentication. Once authentication is successful, the PDS MUST either admit or reject the enrolment request, based on applicable authorization policies. A PDS admitting the enrolment request indicates it via a 2xx-class response, as specified in RFC 3265 [28].

Refer to clauses E.5.2 and E.6.6 for more information on subscription request handling and security requirements, respectively.

3 Enrolment request acceptance

A PDS that admits the enrolment request verifies applicable policies, identifies the requested profile data and prepares a SIP NOTIFY message to the device. Such a notification can either contain the profile data or contain content indirection information that results in the device performing profile content retrieval. The PDS then transmits the prepared SIP notification. When the device successfully receives and accepts the SIP notification, profile enrolment is complete.

When it receives the SIP NOTIFY message, indicating successful profile enrolment, the device SHOULD make the new profile effective within the specified time frame, as described in clause E.6.2. The exception is when the profile data is delivered via content indirection, and the device cannot obtain the profile data within the specified time frame.

Once profile enrolment is successful, the PDS MUST consider the device enrolled for the specific profile, for the duration of the subscription.

E.5.1.2 Content retrieval

A successful profile enrolment leads to an initial SIP notification, and may result in subsequent change notifications. Each of these notifications can either contain profile data, or content indirection information. If it contains content indirection information, the device is required to retrieve the profile data using the specified content retrieval protocols. This process is termed profile content retrieval. For information regarding the use of the SIP NOTIFY message body please refer to clause E.6.5.

Devices and PDSs implementing this framework MUST implement two content retrieval protocols: HTTP and HTTPS as specified in [101] and [102], respectively. Future enhancements or usage of this framework may specify additional or alternative content retrieval protocols. For security requirements and considerations please refer to clause E.5.2.

E.5.1.3 Change notification

Profile data can change over time. Changes can be initiated by various entities (e.g., via the device, back-office components and end-user web interfaces) and for various reasons (e.g., change in user preferences and modifications to services). Profiles may also be shared by multiple devices simultaneously. When a profile is changed the PDS MUST inform all the devices currently enrolled for the specific profile. This process of informing a device of any changes to the profile that it is currently enrolled for is termed change notification.

The PDS provides change notification using a SIP notification (SIP NOTIFY message as specified in RFC 3265 [28]). The SIP notification may provide the changes, a revised profile or content indirection which contains a pointer to the revised data. When a device successfully receives a profile change notification for an enrolled profile, it MUST act upon the changes prior to the expiration of the 'effective-by' parameter.

For NOTIFY content please refer to clause E.6.5.

E.5.1.4 Enrolment data and caching

The requirements for the contents of the SIP SUBSCRIBE used to request profile enrolment are described in this clause. The data required can be configured, cached or discovered – depending on the profile type. If the data is not configured, the device MUST use relevant cached data or proceed with data discovery. This clause describes the requirements for creating a SIP SUBSCRIBE for enrolment, the caching requirements and how data can be discovered.

E.5.1.4.1 Local-network profile

To create a Subscription URI to request the local-network profile a device needs the local network domain name, the device identifier and optionally a user AoR with associated credentials (if one is configured). Since the device can be potentially initialized in a different local-network each time, it SHOULD NOT cache the local network domain, the SIP subscription URI or the local-network profile data across resets. An exception to this is when the device can confirm that it is reinitialized in the same network (using means outside the scope of this document). Thus, in most cases, the device needs to discover the local network domain name. The device discovers this by establishing IP connectivity in the local network (such as via DHCP or pre-configured IP information). Once established, the device MUST attempt to use the local network domain obtained via pre-configuration, if available. If it is not pre- configured, it MUST employ dynamic discovery using DHCPv4 ([b-IETF RFC 2132], Domain Name option) or DHCPv6 (RFC 4704 [107]). Once the local network domain is obtained, the device creates the SIP SUBSCRIBE for enrolment as described below.

- The device MUST NOT populate the user part of the Request-URI. The device MUST set the host portion of the Request-URI to the dot-separated concatenation of "_sipuaconfig" and the local network domain (see example below).
- If the device has been configured with a user AoR for the local network domain (verified as explained in clause E.5.2) it MUST use it to populate the "From" field, unless configured not to (due to privacy concerns, for example). Otherwise, the device MUST set the "From" field to a value of "anonymous@anonymous.invalid".
- The device MUST include the +sip.instance parameter within the 'Contact' header, as specified in [86]. The device MUST ensure that the value of this parameter is the same as that included in any subsequent profile enrolment request.

For example, if the device requested and received the local domain name via DHCP to be: airport.example.net, then the local-network Profile SUBSCRIBE Request-URI would look like: sip:_sipuaconfig.airport.example.net

The local-network profile SUBSCRIBE Request-URI does not have a user part so that the URI is distinct between the "local" and "device" URIs when the domain is the same for the two. This provides a means of routing to the appropriate PDS in domains where there are distinct servers.

The From field is populated with the user AoR, if available. This allows the local network provider to propagate user-specific profile data, if available. The "+sip.instance" parameter within the "Contact" header is set to the device identifier or specifically, the SIP UA instance. Even though every device may get the same (or similar) local-network Profile, the uniqueness of the "+sip.instance" parameter provides an important capability. Having unique instance ID fields allows the management of the local network to track devices present in the network and consequently also manage resources such as bandwidth allocation.

E.5.1.4.2 Device profile type

Once associated with a device, the device provider is not expected to change frequently. Thus, the device is allowed to, and SHOULD cache the Subscription URI for the device profile upon successful enrolment. Exceptions include cases where the device identifier has changed (e.g., new network card), device provider information has changed (e.g., user initiated change) or the device cannot obtain its profile using the Subscription URI. Thus, when available, the device MUST use a cached Subscription URI. If no cached URI is available then it needs to create a Subscription URI. To create a Subscription URI, the device needs a device identity and the device provider's domain name. Unless already configured, the device needs to discover the necessary information and form the subscription URI. In such cases, the following requirements apply for creating a Subscription URI for requesting the device profile:

- The device MUST populate the user part of the Request-URI with the device identifier. The device MUST set the host portion of the Request-URI to the domain name of the device provider. The device identifier format is explained in detail later in this clause.
- The device MUST set the "From" field to a value of anonymous@<device provider's domain>.
- The device MUST include the +sip.instance parameter within the 'Contact' header, as specified in [86]. The device MUST use the same value as the one presented while requesting the local-network profile.

Note that the discovered AoR for the Request-URI can be overridden by a special, provisioned, AoR that is unique to the device. In such cases, the provisioned AoR is used to form the Request-URI and to populate the From field.

If the device is not configured with an AoR, and needs a domain name to populate the Request-URI and the From field, it can either use a configured domain name, if available, or discover it. The options to discover are described below. The device MUST use the results of each successful discovery process for one enrolment attempt, in the order specified below.

- Option 1: Devices that support DHCP MUST attempt to obtain the domain name of the outbound proxy during the DHCP process, using the DHCP option for SIP servers defined in RFC 3361 [103] or RFC 3319 [41] (for IPv4 and IPv6 respectively).
- Option 2: Devices that support DHCP MUST attempt to obtain the local IP network domain during the DHCP process (refer to [b-IETF RFC 2132] and RFC 4704 [107]).
- Option 3: Devices MUST use the local network domain name (configured or discovered to retrieve the local-network profile), prefixing it with the label "_sipuaconfig".

If the device needs to create a subscription URI and needs to use its device identifier, it MUST use the UUID-based URN representation as specified in RFC 4122 [104]. The following requirements apply:

- When the device has a non-alterable MAC address it SHOULD use version 1 UUID representation with the timestamp and clock sequence bits set to a value of '0'. This will allow for easy recognition, and uniqueness of MAC address based UUIDs. An exception is the case where the device supports independent device configuration for more than one SIP UA. An example would be multiple SIP UAs on the same platform.
  - If the device cannot use a non-alterable device identifier, it SHOULD use an alternative non-alterable device identifier, for example, the International Mobile Equipment Identity (IMEI) for mobile devices.
  - If the device cannot use a non-alterable MAC Address, it MUST use the same approach as defining a user agent Instance ID in [86].

NOTE – When the URN is used as the user part of the Request-URI, it MUST be URL escaped since the colon (":") is not a legal character in the user part of an addr-spec (RFC 4122 [104]), and must be escaped.

For example, the instance ID: urn:uuid:f81d4fae-7ced-11d0-a765-00a0c91e6bf6@example.com would be escaped to look as follows in a URI:

sip:urn%3auuid%3af81d4fae-7ced-11d0-a765-00a0c91e6bf6@example.com

The ABNF for the UUID representation is provided in RFC 4122 [104].

E.5.1.4.3 User profile type

To create a Subscription URI to request the user profile on behalf of a user, the device needs to know the user's AoR. This can be statically or dynamically configured on the device (e.g., user input, or propagated as part of the device profile). Similar to device profiles, the content and propagation of user profiles may differ, based on deployment scenarios (i.e., users belonging to the same domain may – or may not – be provided the same profile). To create a subscription URI, the following rules apply:

- The device MUST set the Request-URI to the user AoR.
- The device MUST populate the "From" field with the user AoR.

An authoritative SIP proxy for a SIP provider's network that receives a profile enrolment request for the user profile type will route based on the Event Header field values, thus allowing a subscription to the user's AoR to be routed to the appropriate PDS.

E.5.2 Securing profile delivery

Profile data can contain sensitive information that needs to be secured, such as identities and credentials. Security involves authentication, message integrity and privacy. Authentication is the process by which you verify that an entity is who it claims to be, such as a user AoR presented during profile enrolment. Message integrity provides the assurance that the message contents transmitted between two entities, such as between the PDS and the device, has not been modified during transit. Privacy ensures that the message contents have not been subjected to monitoring by unwanted elements during transit. Authentication and message integrity are required to ensure that the profile contents were received by a valid entity, from a valid source, and without any modifications during transit. For profiles that contain sensitive data, privacy is also required.

For an overview of potential security threats, refer to clause E.9. For information on how the device can be configured with identities and credentials, refer to clause E.5.3.1. The following subclauses provide the security requirements associated with each profile delivery stage, and apply to each of profile types specified by this framework.

E.5.2.1 Securing profile enrolment

Profile enrolment may result in sensitive profile data. In such cases, the PDS MUST authenticate the device, except during the bootstrapping scenario when the device does not have existing credentials (see clause E.5.3.1 for more information on bootstrapping). Additionally, the device MUST authenticate the PDS to ensure that it is obtaining sensitive profile data from a valid PDS.

To authenticate a device that has been configured with identities and credentials as specified in clause E.5.3.1 and support profiles containing sensitive profile data (refer to clause E.5.3.4), devices and PDSs MUST support Digest Authentication as specified in RFC 3261 [26]. Future enhancements may provide other authentication methods such as authentication using X.509 certificates. For the device to authenticate the PDS, the device MUST mutually authenticate with the PDS during digest authentication (device challenges the PDS, which responds with the Authorization header). Transmission of sensitive profile data also requires message integrity. This can be accomplished by configuring the device with, or by ensuring that the discovery process during profile enrolment provides, a SIPS URI resulting in TLS establishment ([81]). TLS also prevents offline dictionary attacks when digest authentication is used. Thus, in the absence of TLS, the device MUST NOT respond to any authentication challenges. It is to be noted that the digest credentials used for obtaining profile data via this framework may, or may not, be the same as that used for SIP registration (see clause E.5.3.1).

When the PDS challenges a profile enrolment request, and it fails, the PDS MAY refuse enrolment or provide profile data without the user-specific information (e.g., to bootstrap a device as indicated in clause E.5.3.1). If the device challenges, but fails to authenticate the PDS, it MUST reject the initial notification and retry the profile enrolment process. If the device is configured with, or discovers, a SIPS URI but TLS establishment fails because the next-hop SIP entity does not support TLS, the device SHOULD attempt other resolved next-hop SIP entities. When the device establishes TLS with the next-hop entity, the device MUST use the procedures specified in RFC 2818 [102], clause E.3.1, for authentication, unless it does not have any configured information (e.g., CA certificate) to perform authentication (like prior to bootstrapping). The 'Server Identity' for authentication is always the domain of the next-hop SIP entity. If the device attempts validation, and it fails, it MUST reject the initial notification and retry profile enrolment. In the absence of a SIPS URI for the device and a mechanism for mutual authentication, the PDS MUST NOT present any sensitive profile data in the initial notification, except when the device is being bootstrapped. It MAY still use content indirection to transmit sensitive profile data.

When a device is being provided with bootstrapping profile data within the notification, and it contains sensitive information, the SIP Identity header SHOULD be used as specified in RFC 4474 [105]. This helps with devices that MAY be pre-configured with certificates to validate bootstrapping sources (e.g., list of allowed domain certificates, or a list of root CA certificates using PKI). When the SIP Identity header is used, the PDS MUST set the host portion of the AoR in the 'From' header to the Provider's domain (the user portion is a entity-specific identifier). If the device is capable of validating the SIP Identity, and it fails, it MUST reject bootstrapping profile data.

E.5.2.2 Securing content retrieval

Initial or change notifications following a successful enrolment can provide a device with the requested profile data, or use content indirection to direct it to a PCC that can provide the profile data. This document specifies HTTP and HTTPS as content retrieval protocols.

If the profile is provided via content indirection and contains sensitive profile data then the PDS MUST use a HTTPS URI for content indirection. PCCs and devices MUST NOT use HTTP for sensitive profile data, except for bootstrapping a device via the device profile. A device MUST authenticate the PCC as specified in RFC 2818 [102], clause E.3.1. A device that is being provided with profile data that contains sensitive data MUST be authenticated using digest authentication as specified in RFC 2617 [21], with the exception of a device that is being bootstrapped for the first time via the device profile. The resulting TLS channel also provides message integrity and privacy.

E.5.2.3 Securing change notification

If the device requested enrolment via a SIP subscription with a non-zero 'Expires' parameter, it can also result in change notifications for the duration of the subscription. For change notifications containing sensitive profile data, this framework RECOMMENDS the use of the SIP Identity header as specified in RFC 4474 [105]. When the SIP Identity header is used, the PDS MUST set the host portion of the AoR in the 'From' header to the Provider's domain (the user portion is a entity-specific identifier). This provides header and body integrity as well. However, for sensitive profile data requiring privacy, if the contact URI to which the NOTIFY request is to be sent is not SIPS, the PDS MUST use content indirection. Additionally, the PDS MUST also use content indirection for notifications containing sensitive profile data, when the profile enrolment was not authenticated.

E.5.3 Additional considerations

This clause provides additional considerations such as details on how a device obtains identities and credentials, backoff and retry methods, guidelines on profile data, and additional profile types.

E.5.3.1 Bootstrapping identities and credentials

When requesting a profile the profile delivery server will likely require the device to provide an identity (i.e., a user AoR), and associated credentials for authentication. During this process (e.g., digest authentication), the PDS is also required to present its knowledge of the credentials to ensure mutual authentication (see clause E.5.2.1). For mutual authentication with the PDS, the device needs to be provided with the necessary identities and credentials (e.g., username/password, certificates). This is done via bootstrapping. For a discussion around the security considerations related to bootstrapping, please see clause E.9.2.

Bootstrapping a device with the required identities and credentials can be accomplished in one of the following ways:

Pre-configuration

The device may be pre-configured with identities and associated credentials, such as a user AoR and digest password.

Out-of-band methods

A device or Provider may provide hardware- or software-based credentials such as SIM cards or Universal Serial Bus (USB) drives.

End-user interface

The end-user may be provided with the necessary identities and credentials. The end-user can then configure the device (using a user interface), or present when required (e.g., IM login screen).

Using this framework

When a device is initialized, even if it has no pre-configured information, it can request the local-network and device profiles. For purposes of bootstrapping, this framework recommends that the device profile provide one of the following to bootstrap the device:

- Profile data that allows the end-user to communicate with the device provider or SIP service provider using non-SIP methods. For example, the profile data can direct the end-user to a web portal to obtain a subscription. Upon obtaining a successful subscription, the end-user or the device can be provided with the necessary identities and credentials.
- Content indirection information to a PCC that can provide identities and credentials. As an example, consider a device that has a X.509 certificate that can be authenticated by the PCC. In such a case, the PCC can use HTTPS to provide identities and associated credentials.
- Profile data containing identities and credentials that can be used to bootstrap the device (see clause E.5.3.4 for profile data recommendations). This can be used in cases where the device is initialized for the first time, or after a factory reset. This can be considered only in cases where the device is initialized in the Provider's network, for obvious security reasons.

Additionally, AoRs are typically known by PDSs that serve the domain indicated by the AoR. Thus, devices can only present the configured AoRs in the respective domains. An exception is the use of federated identities. This allows a device to use a user's AoR in multiple domains. Further even within the same domain, the device's domain proxy and the PDS may be in two different realms, and as such may be associated with different credentials for digest authentication. In such cases, multiple credentials may be configured, and associated with the realms in which they are to be used.

This framework specifies only digest authentication for profile enrolment and the device is not expected to contain any other credentials. For profile retrieval using content indirection, the device will need to support additional credentials such as X.509 certificates (for TLS). Future enhancements can specify additional credential types for profile enrolment and retrieval.

E.5.3.2 Profile enrolment request attempt

A state diagram representing a device requesting any specific profile defined by this framework is shown in Figure E.6.

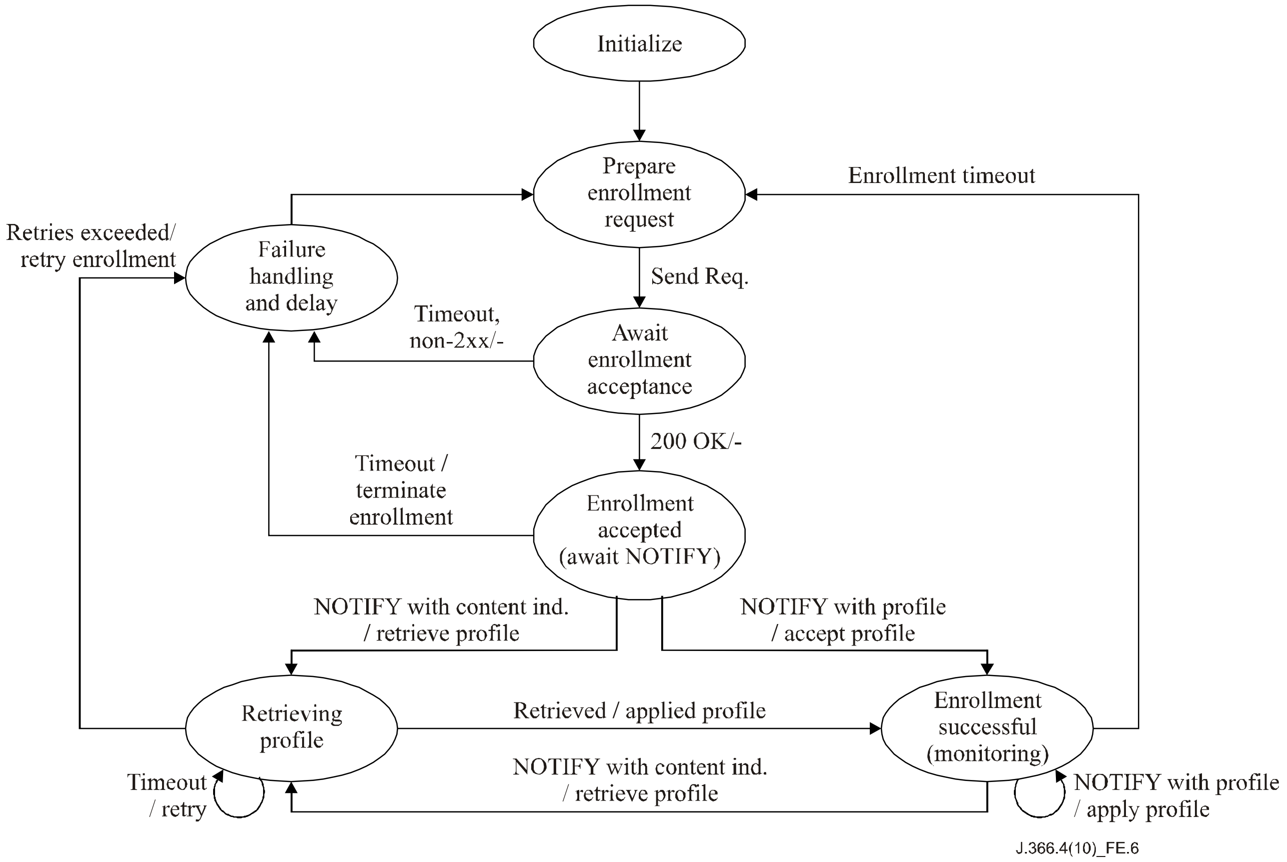
Initialize
Prepare enrollment request
Enrollment timeout
Retries exceeded/ retry enrollment
Failure handling and delay
Send Req.
Timeout, non-2xx/-
Await enrollment acceptance
200 OK/-
Timeout / terminate enrollment
Enrollment accepted (await NOTIFY)
NOTIFY with content ind. / retrieve profile
NOTIFY with profile / accept profile
Retrieving profile
Retrieved / applied profile
Enrollment successful (monitoring)
Timeout / retry
NOTIFY with content ind. / retrieve profile
NOTIFY with profile / apply profile
J.366.4(10)_FE.6

Figure E.6 – Device state diagram

As a reminder:

- The timeout for SIP messages is specified by RFC 3261 [26]. In the cases where this is not specified such as the timeout to wait for the initial notification during profile enrolment, it is left to device implementations or future protocol enhancements.
- The timeout for profile retrieval using content indirection will be as specified by profile retrieval protocols employed. If none exists, it is left to device implementations.

In addition, since profile enrolment is a process unique to this framework, the device MUST follow the enrolment attempt along with exponential backoff and retry mechanisms as indicated in Figure E.7.

```
Function for Profile Enrolment ()
 Init Function: Iteration i=0
 Loop 1: Attempt
    Loop 2: For each SIP Subscription URI
      Loop 3: For each next-hop SIP entity
        - Prepare & transmit Enrolment Request
        - Await Enrolment Acceptance and initial NOTIFY
```

```
         + If the profile enrolment is successful
          = Exit this function()
         + If profile enrolment fails due to an explicit
          failure or a timeout as specified in RFC3261
          = Continue with the next-hop SIP entity (Loop 3)
       End Loop: Loop 3
     End Loop: Loop 2
     (Note: If you are here, profile enrolment did not succeed)
     + Is any valid cached profile data available?
      = If yes, use it and continue with Loop 1
     + If the enrolment request is for a non-mandatory profile
      = Start profile enrolment for the next profile,
       if applicable
     - Delay for 2^i*(64*T1); -- this is exponential backoff
     - increment i;
     - If i>8, reset i=8;
    End loop: Loop 1
  End Function()
```

Figure E.7 – Profile enrolment attempt (pseudo-code)

The pseudo-code above (Figure E.7) allows for cached profiles to be used. However, any cached Local Network profile MUST NOT be used unless the device can ensure that it is in the same local network which provided the cached data. This framework does not provide any procedures for local network recognition. Any cached device and user profiles MUST only be used in domains that they are associated with. For example, a cached device profile is used only when the associated domain matches the current device provider's domain. If a PDS wants to invalidate a profile it may do so by transmitting a NOTIFY with an 'empty profile', i.e., profile instance without any included data (if supported by the profile data model; not to be confused with an empty NOTIFY), or via an explicit profile data element that invalidates the data. A device receiving such a NOTIFY MUST discard the applicable profile (i.e., it cannot even store it in the cache). Additionally, if a factory reset is available and performed on a device, it MUST reset the device to its initial state prior to any configuration. Specifically, the device MUST set the device back to the state when it was originally distributed.

The order of profile enrolment is important. For the profiles specified in this framework, the device must enrol in the following default order: local-network, device and user. The pseudo-code presented earlier (Figure E.7) differentiates between 'mandatory' and 'non-mandatory' profiles. This distinction is left to profile data definitions.

It is to be noted that this framework does not allow the devices to inform the PDSs of profile retrieval errors such as invalid data. Follow-on standardization activities are expected to address this feature.

E.5.3.3 Device types

The examples in this framework tend to associate devices with entities that are accessible to end-users. However, this is not necessarily the only type of device that can utilize the specified Framework. Devices can be entities such as SIP Phones or soft clients, with or without user interfaces (that allow for device Configuration), entities in the network that do not directly communicate with any users (e.g., gateways, media servers, etc) or network infrastructure elements e.g., SIP servers).

E.5.3.4 Profile data

This framework does not specify the contents for any profile type. Follow-on standardization activities are expected to address profile contents. However, the framework provides the following requirements and recommendations for profile data definitions:

- The device profile type SHOULD specify parameters to configure the identities and credentials for use in scenarios such as bootstrapping (see clause E.5.3.1) and run-time modifications to identities and credentials. This framework recommends the device profile to provide the identities and credentials due to a couple of reasons. The local-network profile may not always be available, and even if present, may not be controlled by the device provider who controls device configuration to provide services. Further, the device may not have any users configured prior to being bootstrapped, resulting in an absence of user profile requests. However, this framework does not prevent other profile types from providing identities and credentials to meet deployment needs. For example, the user profile can contain identities and credentials for communicating with specific applications.
- Each profile MUST clearly identify if it may contain any sensitive data. Such profiles MUST also identify the data elements that are considered sensitive, i.e., data that cannot be compromised. As an example, a device profile definition may identify itself as containing sensitive data and indicate data such as device credentials to be sensitive.
- When the device receives multiple profiles, the contents of each profile type SHOULD only contain data relevant to the entity it represents. As an example, consider a device that obtains all the defined profiles. Information pertaining to the local network is contained in the 'local-network' profile and not the 'user' profile. This does not preclude relevant data about a different entity from being included in a profile type, e.g., the 'device' profile type may contain information about the users allowed to access services via the device. A profile may also contain starting information to obtain subsequent Profiles.
- Data overlap SHOULD be avoided across profile types, unless necessary. If data overlap is present, prioritization of the data is left to data definitions. As an example, the device profile may contain the list of codecs to be used by the device and the user Profile (for a user on the device) may contain the codecs preferred by the user. Thus, the same data (usable codecs) is present in two profiles. However, the data definitions may indicate that to function effectively, any codec chosen for communication needs to be present in both the profiles.

E.5.3.5 Profile data frameworks

The framework specified in this document does not address profile data representation, storage or retrieval protocols. It assumes that the PDS has a PCC based on existing or other Profile Data Frameworks.

While this framework does not impose specific constraints on any such framework, it does allow for the propagation of profile content to the PDS (specifically the PCC) from a network element or the device. Thus, Profile Data or Retrieval frameworks used in conjunction with this framework MAY consider techniques for propagating incremental, atomic changes to the PDS. One means for propagating changes to a PDS is defined in XCAP ([b-IETF RFC 4825]).

E.5.3.6 Additional profile types

This document specifies three profile types: local-network, device and user. However, there may be use cases for additional profile types. e.g., profile types for application specific profile data or to provide enterprise-specific policies. Definition of such additional profile types is not prohibited, but considered out of scope for this document. Such profile definitions MUST specify the order of retrieval with respect to all the other profiles such as the local-network, device and user profile types defined in this document.

E.5.3.7 Deployment considerations

The framework defined in this document was designed to address various deployment considerations, some of which are highlighted below.

Provider relationships:

- The local network provider and the SIP service provider can often be different entities, with no administrative or business relationship with each other.
- There may be multiple SIP service providers involved, one for each service that a user subscribes to (telephony service, instant messaging, etc.); this Framework does not specify explicit behaviour in such a scenario, but it does not prohibit its usage either.
- Each user accessing services via the same device may subscribe to different sets of services, from different Service Providers.

User-device relationship:

- The relationship between devices and users can be many-to-many (e.g., a particular device may allow for many users to obtain subscription services through it, and individual users may have access to multiple devices).
- Each user may have different preferences for use of services, and presentation of those services in the device user interface.
- Each user may have different personal information applicable to use of the device, either as related to particular services, or independent of them.

E.5.4 Support for NATs

PDSs that support devices behind NATs, and devices that can be behind NATs can use procedures specified in [86]. The Outbound proxies can be configured or discovered. Clients that support such behaviour MUST include the 'outbound' option-tag in a Supported header field value, and add the "ob" parameter as specified in [86] within the SIP SUBSCRIBE for profile enrolment.

E.6 Event package definition

The framework specified in this document proposes and specifies a new SIP Event Package as allowed by RFC 3265 [28]. The purpose is to allow for devices to subscribe to specific profile types with PDSs and for the PDSs to notify the devices with the profile data or content indirection information.

The requirements specified in RFC 3265 [28] apply to this package. The following sub-sections specify the Event Package description and the associated requirements. The framework requirements are defined in clause E.5.

E.6.1 Event package name

The name of this package is "ua-profile". This value appears in the Event header field present in SUBSCRIBE and NOTIFY requests for this package as defined in RFC 3265 [28].

E.6.2 Event package parameters

This package defines the following new parameters for the event header:

"profile-type", "vendor", "model", "version", and "effective-by"

The following rules apply:

- All the new parameters, with the exception of the "effective-by" parameter MUST only be used in SUBSCRIBE requests and ignored if they appear in NOTIFY requests.
- The "effective-by" parameter is for use in NOTIFY requests only and MUST be ignored if it appears in SUBSCRIBE requests.

The semantics of these new parameters are specified in the following subclauses.

E.6.2.1 profile-type

The "profile-type" parameter is used to indicate the token name of the profile type the user agent wishes to obtain and to be notified of subsequent changes. This document defines three logical types of profiles and their token names. They are as follows:

- *local-network*: specifying the "local-network" type profile indicates the desire for profile data, and potentially, profile change notifications specific to the local network.
- *device*: specifying the "device" type profile(s) indicates the desire for the profile data, and potentially, profile change notification that is specific to the device or user agent.
- *user*: Specifying "user" type profile indicates the desire for the profile data, and potentially, profile change notification specific to the user.

The profile type is identified in the Event header parameter: "profile-type". A separate SUBSCRIBE dialog is used for each profile type. Thus, the subscription dialog on which a NOTIFY arrives implies which profile's data is contained in, or referred to, by the NOTIFY message body. The Accept header of the SUBSCRIBE request MUST include the MIME types for all profile content types for which the subscribing user agent wishes to retrieve profiles, or receive change notifications.

In the following syntax definition using ABNF, EQUAL and token are defined in RFC 3261 [26]. It is to be noted that additional profile types may be defined in subsequent documents.

```
Profile-type  = "profile-type" EQUAL profile-value
profile-value = profile-types / token
profile-types = "device" / "user" / "local-network"
```

The "device", "user" or "local-network" token in the profile-type parameter may represent a class or set of profile properties. Follow-on standards defining specific profile contents may find it desirable to define additional tokens for the profile-type parameter. Also, additional content types may be defined along with the profile formats that can be used in the Accept header of the SUBSCRIBE to filter or indicate what data sets of the profile are desired.

E.6.2.2 vendor, model and version

The "vendor", "model" and "version" parameter values are tokens specified by the implementer of the user agent. These parameters MUST be provided in the SUBSCRIBE request for all profile types. The implementer SHOULD use their DNS domain name (e.g., example.com) as the value of the "vendor" parameter so that it is known to be unique. These parameters are useful to the PDS to affect the profiles provided. In some scenarios it is desirable to provide different profiles based upon these parameters. e.g., feature property X in a profile may work differently on two versions of the same user agent. This gives the PDS the ability to compensate for or take advantage of the differences. In the following ABNF defining the syntax, EQUAL and quoted-string are defined in RFC 3261 [26].

```
Vendor = "vendor" EQUAL quoted-string
Model = "model" EQUAL quoted-string
Version = "version" EQUAL quoted-string
```

E.6.2.3 effective-by parameter

The "effective-by" parameter in the Event header of the NOTIFY request specifies the maximum number of seconds before the user agent must attempt to make the new profile effective. The "effective-by" parameter MAY be provided in the NOTIFY request for any of the profile types. A value of 0 (zero) indicates that the subscribing user agent must attempt to make the profiles effective immediately (despite possible service interruptions). This gives the PDS the power to control when the profile is effective. This may be important to resolve an emergency problem or disable a user agent immediately. If it is absent, the device SHOULD attempt to make the profile data effective at the earliest possible opportunity that does not disrupt any services being offered. The "effective-by" parameter is ignored in all messages other than the NOTIFY request. In the following ABNF, EQUAL and DIGIT are defined in RFC 3261 [26].

```
Effective-By = "effective-by" EQUAL 1*DIGIT
```

E.6.2.4 Summary of event parameters

The following are example Event headers which may occur in SUBSCRIBE requests. These examples are not intended to be complete SUBSCRIBE requests.

```
Event: ua-profile;profile-type=device;
     vendor="vendor.example.com";model="Z100";version="1.2.3"
Event: ua-profile;profile-type=user;
     vendor="premier.example.com";model="trs8000";version="5.5"
```

The following are example Event headers which may occur in NOTIFY requests. These example headers are not intended to be complete SUBSCRIBE requests.

```
Event: ua-profile;effective-by=0
Event: ua-profile;effective-by=3600
```

The following table shows the use of Event header parameters in SUBSCRIBE requests for the three profile types:

profile-type	device	user	local-network
vendor	m	m	m
model	m	m	m
version	m	m	m
effective-by			
m – mandatory s – SHOULD be provided o – optional			

Non-specified means that the parameter has no meaning and should be ignored.

The following table shows the use of Event header parameters in NOTIFY requests for the three profile types:

profile-type	device	user	local-network
vendor			
model			
version			
effective-by	o	o	o
m – mandatory s – SHOULD be provided o – optional			

E.6.3 SUBSCRIBE bodies

This package defines no use of the SUBSCRIBE request body. If present, it SHOULD be ignored. Exceptions include future enhancements to the framework which may specify a use for the

SUBSCRIBE request body.

E.6.4 Subscription duration

The duration of a subscription is specific to SIP deployments and no specific recommendation is made by this Event Package. If absent, a value of 86400 seconds (24 hours; 1 day) is RECOMMENDED since the presence (or absence) of a device subscription is not time critical to the regular functioning of the PDS.

It is to be noted that a one-time fetch of a profile, without ongoing subscription, can be accomplished by setting the 'Expires' parameter to a value of Zero, as specified in RFC 3265 [28].

E.6.5 NOTIFY bodies

The framework specifying the Event Package allows for the NOTIFY body to contain the profile data, or a pointer to the profile data using content indirection. For profile data delivered via content indirection, i.e., a pointer to a PCC, then the Content-ID MIME header, as described in RFC 4483 [106] MUST be used for each Profile document URI. At a minimum, the "http:" [101] and "https:" RFC 2818 [102] URI schemes MUST be supported; other URI schemes MAY be supported based on the Profile Data Frameworks (examples include FTP [b-IETF RFC 959], LDAP [b-IETF RFC 4510] and XCAP [b-IETF RFC 4825]).

A non-empty NOTIFY body MUST include a MIME type specified in the 'Accept' header of the SUBSCRIBE. Further, if the Accept header of the SUBSCRIBE included the MIME type message/external-body (indicating support for content indirection) then the PDS MAY use content indirection in the NOTIFY body for providing the profiles.

E.6.6 Notifier processing of SUBSCRIBE requests

A successful SUBSCRIBE request results in a NOTIFY with either profile contents or a pointer to it (via Content Indirection). The SUBSCRIBE SHOULD be either authenticated, or transmitted over an integrity protected SIP communications channel. Exceptions include cases where the identity of the Subscriber is unknown and the Notifier is configured to accept such requests.

The Notifier MAY also authenticate SUBSCRIBE messages even if the NOTIFY is expected to only contain a pointer to profile data. Securing data sent via Content Indirection is covered in clause E.9.

If the profile type indicated in the "profile-type" Event header parameter is unavailable or the Notifier is configured not to provide it, the Notifier SHOULD return a 404 response to the SUBSCRIBE request. If the specific user or device is unknown, the Notifier MAY accept the subscription, or else it may reject the subscription (with a 403 response).

E.6.7 Notifier generation of NOTIFY requests

As specified in RFC 3265 [28], the Notifier MUST always send a NOTIFY request upon accepting a subscription. If the device or user is unknown and the Notifier chooses to accept the subscription, the Notifier MAY either respond with profile data (e.g., default profile data) or provide no profile information (i.e., empty NOTIFY).

If the identity indicated in the SUBSCRIBE request (From header) is a known identity and the requested profile information is available (i.e. as specified in the profile-type parameter of the Event header), the Notifier SHOULD send a NOTIFY with profile data. Profile data MAY be sent as profile contents or via Content Indirection (if the content indirection MIME type was included in the Accept header). The Notifier MUST NOT use any scheme that was not indicated in the "schemes" Contact header field.

The Notifier MAY specify when the new profiles must be made effective by the Subscriber by specifying a maximum time in seconds (zero or more) in the "effective-by" event header parameter.

If the SUBSCRIBE was received over an integrity protected SIP communications channel, the Notifier SHOULD send the NOTIFY over the same channel.

E.6.8 Subscriber processing of NOTIFY requests

A Subscriber to this event package MUST adhere to the NOTIFY request processing behaviour specified in RFC 3265 [28]. If the Notifier indicated an effective time (using the "effective-by" Event Header parameter), the Subscriber SHOULD attempt to make the profiles effective within the specified time. Exceptions include deployments that prohibit such behaviour in certain cases (e.g., emergency sessions are in progress). When profile data cannot be applied within the recommended time frame and this affects device behaviour, any actions to be taken SHOULD be defined by the profile data definitions. By default, the Subscriber is RECOMMENDED to make the profiles effective as soon as possible.

When accepting content indirection, the Subscriber MUST always support "http:" or "https:" and be prepared to accept NOTIFY messages with those URI schemes. If the Subscriber wishes to support alternative URI schemes they MUST each be indicated in the "schemes" Contact header field parameter as defined in RFC 4483 [106]. The Subscriber MUST also be prepared to receive a NOTIFY request with no body. The subscriber MUST NOT reject the NOTIFY request with no body. The subscription dialog MUST NOT be terminated by a empty NOTIFY, i.e., with no body.

E.6.9 Handling of forked requests

This Event package allows the creation of only one dialog as a result of an initial SUBSCRIBE request as described in section 4.4.9 of RFC 3265 [28]. It does not support the creation of multiple subscriptions using forked SUBSCRIBE requests.

E.6.10 Rate of notifications

The rate of notifications for the profiles in this framework is deployment specific, but expected to be infrequent. Hence, the Event Package specification does not specify a throttling or minimum period between NOTIFY requests.

E.6.11 State agents

State agents are not applicable to this Event Package.

E.7 Examples

This clause provides examples along with sample SIP message bodies relevant to this framework. Both the examples are derived from the use case illustrated in clause E.4.1, specifically the request for the device profile. The examples are informative only.

E.7.1 Example 1: Device requesting profile

This example illustrates the detailed message flows between the device and the SIP Service Provider's network for requesting and retrieving the profile (the flow uses the device profile as an example).

The following are assumed for this example:

- Device is assumed to have established local network connectivity; NAT and Firewall considerations are assumed to have been addressed by the SIP Service Provider.
- Examples are snapshots only and do not illustrate all the interactions between the device and the Service Provider's network (and none between the entities in the SIP Service Provider's network).
- All SIP communication with the SIP Service Provider happens via a SIP Proxy.
- HTTP over TLS is assumed to be the Content Retrieval method used (any suitable alternative can be used as well).

The flow diagram and an explanation of the messages follow.

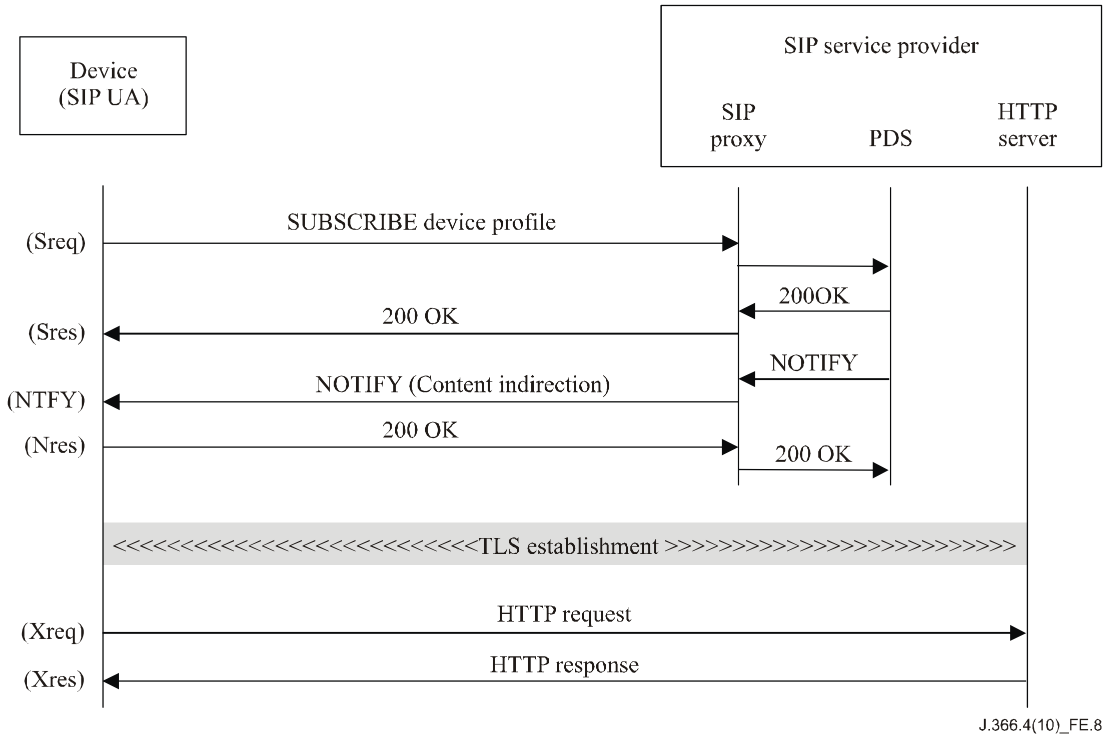

Figure E.8 – message flow diagram for device requesting profile

(SReq) The device transmits a request for the 'device' profile using the SIP SUBSCRIBE utilizing the Event Package specified in this framework.

NOTE 1 – Some of the header fields (e.g., SUBSCRIBE, Event, via) are continued on a separate line due to format constraints of this document.

```
SUBSCRIBE sip:urn%3auuid%3a00000000-0000-1000-0000-00FF8D82EDCB
     @example.com SIP/2.0
Event: ua-profile;profile-type=device;vendor="vendor.example.net";
   model="Z100";version="1.2.3"
From: anonymous@example.com;tag=1234
To: sip:urn%3auuid%3a00000000-0000-1000-0000-00FF8D82EDCB@example.com
Call-ID: 3573853342923422@192.0.2.44
CSeq: 2131 SUBSCRIBE
Contact: sip:urn%3auuid%3a00000000-0000-1000-0000-00FF8D82EDCB
 @192.168.1.44
 ;+sip.instance="<urn:uuid:00000000-0000-0000-0000-123456789AB0>"
 ;schemes="http,https"


Via: SIP/2.0/TCP 192.0.2.41;
 branch=z9hG4bK6d6d35b6e2a203104d97211a3d18f57a
Accept: message/external-body, application/x-z100-device-profile
Content-Length: 0
```

(SRes) The SUBSCRIBE request is received by a SIP Proxy in the Service Provider's network which transmits it to the PDS. The PDS accepts the response and responds with a 200 OK.

NOTE 2 – The device and the SIP proxy may have established a secure communications channel (e.g., TLS).

(NTFY) Subsequently, the PDS transmits a SIP NOTIFY message indicating the profile location.

NOTE 3 – Some of the fields (e.g., content-type) are continued on a separate line due to format constraints of this document.

```
NOTIFY sip:urn%3auuid%3a00000000-0000-1000-0000-00FF8D82EDCB
     @192.168.1.44 SIP/2.0
 Event: ua-profile;effective-by=3600
 From: sip:urn%3auuid%3a00000000-0000-1000-0000-00FF8D82EDCB@example.com
    ;tag=abca
 To: sip:urn%3auuid%3a00000000-0000-1000-0000-00FF8D82EDCB@example.com
   ;tag=1234
 Call-ID: 3573853342923422@192.0.2.44
 CSeq: 322 NOTIFY
 Via: SIP/2.0/UDP 192.0.2.3;
  branch=z9hG4bK1e3effada91dc37fd5a0c95cbf6767d0
 MIME-Version: 1.0
 Content-Type: message/external-body; access-type="URL";
        expiration="Mon, 01 Jan 2010 09:00:00 UTC";
        URL="http://example.com/z100-000000000000.html";
        size=9999;
        hash=10AB568E91245681AC1B

 Content-Type: application/x-z100-device-profile
 Content-ID: <39EHF78SA@example.com>
 .
 .
 .
```

(NRes) Device accepts the NOTIFY message and responds with a 200 OK.

(XReq) Once the necessary secure communications channel is established, the device sends an HTTP request to the HTTP server indicated in the NOTIFY.

(XRes) The HTTP server responds to the request via a HTTP response containing the profile contents.

E.7.2 Example 2: Device obtaining change notification

The following example illustrates the case where a user (X) is simultaneously accessing services via two different devices (e.g., Multimedia entities on a PC and PDA) and has access to a user interface that allows for changes to the user profile.

The following are assumed for this example:

- The devices (A & B) obtain the necessary profiles from the same SIP Service Provider.
- The SIP Service Provider also provides a user interface that allows the user to change preferences that impact the user profile.

The flow diagram is shown in Figure E.9 and an explanation of the messages follows the figure.

NOTE 1 – The example only shows retrieval of user X's profile, but it may request and retrieve other profiles (e.g., local-network, Device).

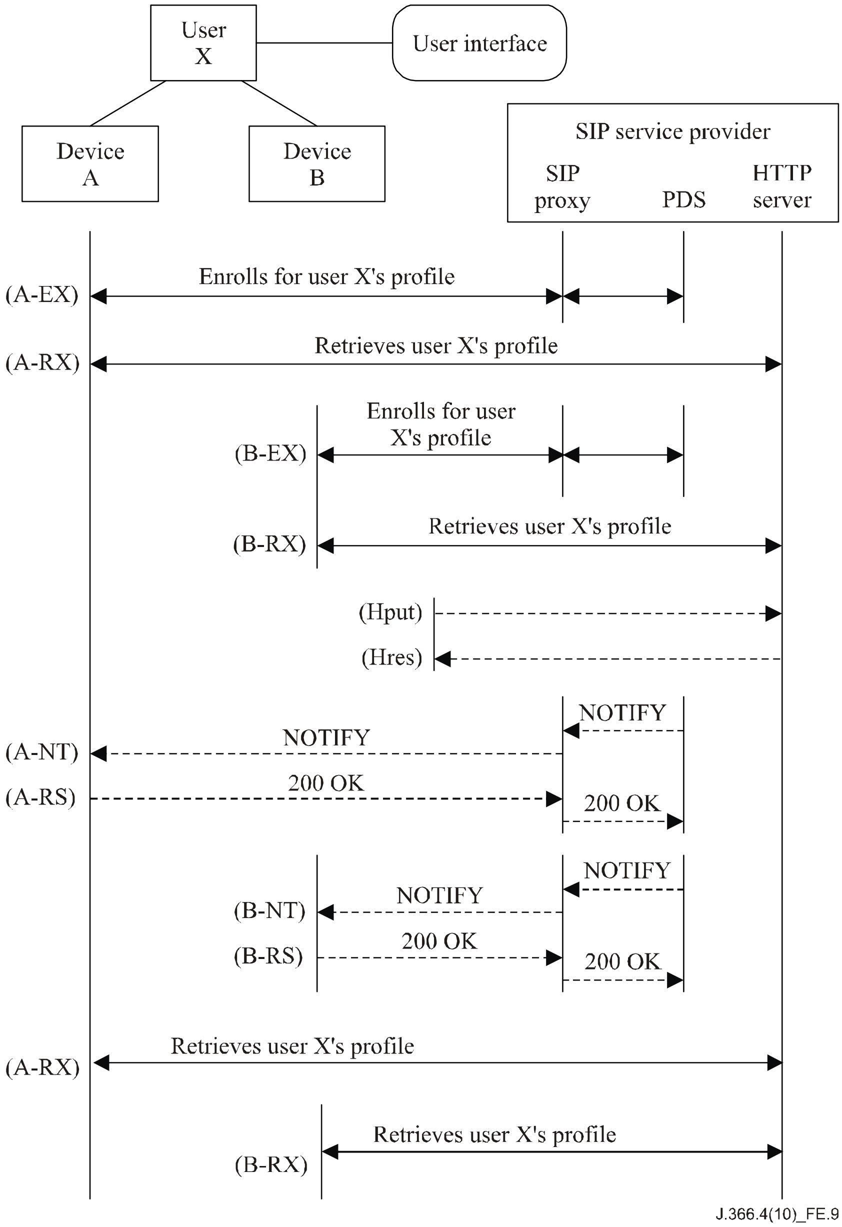

Figure E.9 – Message flow diagram for device obtaining change notification

(A-EX) Device A discovers, enrols and obtains notification related to user X's profile.

(A-RX) Device A retrieves user X's profile.

(B-EX) Device B discovers, enrols and obtains notification related to user X's profile.

(B-RX) Device B retrieves user X's profile.

(HPut) Changes affected by the user via the user interface are uploaded to the HTTP Server.

NOTE 2 – The UI itself can act as a device and subscribe to user X's profile. This is not the case in the example shown.

(HRes) Changes are accepted by the HTTP server.

(A-NT) PDS transmits a NOTIFY message to device A indicating the changed profile. A sample message is shown below:

NOTE 3 – Some of the fields (e.g., Via) are continued on a separate line due to format constraints of this document.

```
NOTIFY sip:userX@192.0.2.44 SIP/2.0
Event: ua-profile;effective-by=3600
From: sip:userX@sip.example.net;tag=abcd
To: sip:userX@sip.example.net.net;tag=1234
Call-ID: 3573853342923422@192.0.2.44
CSeq: 322 NOTIFY
Via: SIP/2.0/UDP 192.0.2.3;
 branch=z9hG4bK1e3effada91dc37fd5a0c95cbf6767d1
MIME-Version: 1.0
Content-Type: message/external-body; access-type="URL";
       expiration="Mon, 01 Jan 2010 09:00:00 UTC";
       URL="http://www.example.com/user-x-profile.html";
       size=9999;
       hash=123456789AAABBBCCCDD
.
.
.
```

(A-RS) Device A accepts the NOTIFY and sends a 200 OK

(B-NT) PDS transmits a NOTIFY message to device B indicating the changed profile. A sample message is shown below:

NOTE 4 – Some of the fields (e.g., Via) are continued on a separate line due to format constraints of this document.

```
NOTIFY sip:userX@192.0.2.43 SIP/2.0
Event: ua-profile;effective-by=3600
From: sip:userX@sip.example.net;tag=abce
To: sip:userX@sip.example.net.net;tag=1234
Call-ID: 3573853342923422@192.0.2.43
CSeq: 322 NOTIFY
Via: SIP/2.0/UDP 192.0.2.3;
 branch=z9hG4bK1e3effada91dc37fd5a0c95cbf6767d2
MIME-Version: 1.0
Content-Type: message/external-body; access-type="URL";
       expiration="Mon, 01 Jan 2010 09:00:00 UTC";
       URL="http://www.example.com/user-x-profile.html";
       size=9999;
       hash=123456789AAABBBCCCDD
.
.
.
```

(B-RS) Device B accepts the NOTIFY and sends a 200 OK

(A-RX) Device A retrieves the updated profile pertaining to user X

(B-RX) Device B retrieves the updated profile pertaining to user X

E.8 IANA considerations

There are two IANA considerations associated with the contents of this Annex, SIP event package and SIP configuration profile types. These considerations are being pursued through activities within IETF.

E.9 Security considerations

The framework specified in this document specifies profile delivery stages, an event package and three profile types to enable profile delivery. The profile delivery stages are: enrolment, content retrieval, and change notification. The event package helps with enrolment and change notifications. Each profile type allows for profile retrieval from a PDS belonging to a specific provider.

Enrolment allows a device to request, and if successful, to enrol with a PDS to obtain profile data. To transmit the request the device relies on configured, cached or discovered data. Such data includes provider domain names, identities, and credentials. The device either uses configured outbound proxies or discovers the next-hop entity using RFC 3263 [27A] that can result in a SIP proxy or the PDS. It then transmits the request. A SIP Proxy receiving the request uses the Request-URI and event header contents to route it to a PDS (via other SIP proxies, if required).

When a PDS receives the enrolment request, it can either challenge any contained identity or admit the enrolment. Authorization rules then decide if the enrolment gets accepted. If accepted, the PDS sends an initial notification that contains either the profile data, or content indirection information. The profile data can contain generic profile data (common across multiple devices) or information specific to an entity (such as the device or a user). If specific to an entity, it may contain sensitive information such as credentials. Compromise of sensitive data can lead to threats such as impersonation attacks (establishing rogue sessions), theft of service (if services are obtainable), and zombie attacks. It is important for the device to ensure the authenticity of the PNC and the PCC since impersonation of the SIP service provider can lead to Denial of Service and Man-in-the-Middle attacks.

Profile content retrieval allows a device to retrieve profile data via content indirection from a PCC. This communication is accomplished using one of many profile delivery protocols or frameworks, such as HTTP or HTTPS as specified in this document. However, since the profile data returned is subject to the same considerations as that sent via profile notification, similar threats exist: for example, denial of service attacks (rogue devices bombard the PCC with requests for a specific profile) and attempts to modify erroneous data onto the PCC (since the location and format may be known). Thus, for the delivery of any sensitive profile data, authentication of the entity requesting profile data is required. It is also important for the requesting entity to authenticate the profile source via content indirection, and ensure that the sensitive profile data is protected via message integrity. For sensitive data that should not be subject to snooping, privacy is also required.

The following clauses highlight the security considerations that are specific to each profile type.

E.9.1 Local-network profile

A local network may or may not (e.g., home router) support local- network profiles as specified in this framework. Even if supported, the PDS may only be configured with a generic local-network profile that is provided to every device that requests the local-network profile. Such a PDS may not implement any authentication requirements or TLS.

Alternatively, certain deployments may require the entities – device and the PDS – to authenticate each other prior to successful profile enrolment. Such networks may pre-configure user identities to the devices and allow user-specific local-network profiles. In such networks the PDS will support digest, and the devices are configured with user identities and credentials as specified in clause E.5.3.1. If sensitive profile data is being transmitted, the user identity is a SIPS URI that results in TLS with the next-hop (which is authenticated), and digest authentication is used by the PDS and the device.

This framework supports both use cases and any variations in-between. However, devices obtaining local-network profiles from an unauthenticated PDS are cautioned against potential Man-in-the-Middle or PDS impersonation attacks. This framework requires that a device reject sensitive data, such as credentials, from unauthenticated local-network sources. It also prohibits devices from responding to authentication challenges in the absence of TLS on all hops as a result of using a SIPS URI. Responding to unauthenticated challenges allows for dictionary attacks that can reveal weak passwords. The only exception to accepting such sensitive data without authentication of the PDS is in the case of bootstrapping (see clause E.5.3.1). In the case of bootstrapping, the methods employed need to be aware of potential security threats such as impersonation.

The use of SIP Identity is useful for the device to validate notifications in the absence of a secure channel such as TLS when a SIPS URI is used. In such cases the device can validate the SIP Identity header to verify the source of the profile notification, and the source of the profile data when content indirection is not used. However, the presence of the header does not guarantee the validity of the data. It verifies the source and confirms data integrity, but the data obtained from an undesired source may still be invalid, e.g., invalid outbound proxy information, resulting in Denial of Service. Thus, devices requesting the local-network profile from unknown networks need to be prepared to discard information that prevent retrieval of other, required, profiles.

E.9.2 Device profile

Device profiles deal with device-specific configuration. They may be provided to unknown devices that are attempting to obtain profiles for purposes such as trials, self-subscription (not to be confused with RFC 3265 [28]) and emergency services.

This framework allows for the device profile to be used for bootstrapping a device. Such bootstrapping profile data may contain enough information to connect to a Provider. For example, it may enable the device to communicate with a device provider, allowing for trial or self-subscription services via visual or audio interfaces (e.g., interactive voice response), or customer service representatives. The profile data may also allow the device a choice of device providers and allow the end-user to choose one. The profile data may also contain identities and credentials (temporary or long-term) that can be used to obtain further profile data from the network. This framework recommends the use of the SIP Identity header by the PDS. However, to be able to validate the SIP Identity header, the device needs to be pre-configured with the knowledge of allowable domains or certificates for validation (e.g., using PKI). If not, the device can still guarantee header and body integrity if the profile data contains the domain certificate (but the data can still be invalid or malicious). In such cases, devices supporting user interfaces may obtain confirmation from the user trying to bootstrap the device (confirming header and body integrity). However, when the SIP Identity header is not present, or the device is not capable of validating it, the bootstrapping data is unauthenticated and obtained without any integrity protection. Such bootstrapping data, however, may contain only temporary credentials (SIPS URI and digest credentials) that can be used to reconnect to the network to ensure message integrity and privacy prior to obtaining long-term credentials. It is to be noted that such devices are at the mercy of the network they request the device profile from. If they are initialized in a rogue network, or get hijacked by a rogue PDS, the end-user may be left without desired device operation or, worse, unwanted operation. To mitigate such factors the device provider may communicate temporary credentials (e.g., passwords that can be entered via an interface) or permanent credentials (e.g., a USB device) to the end-user for connectivity. If such methods are used, those credentials MUST be quickly replaced by largeentropy credentials, to minimize the impact of dictionary attacks. Future enhancements to this framework may specify device capabilities that allow for authentication without any provider specific configuration (e.g., X.509 certificates using PKI can allow for authentication by any provider with access to the CA certificate). Alternatively, the device may be pre-configured with credentials for use with content indirection mechanisms. In such circumstances a PDS can use secure content indirection mechanism, such as HTTPS, to provide the bootstrapping data.

Once a device is associated with a device provider the device profile is vital to device operation. This is because the device profile can contain important operational information such as users that are to be allowed access (white-list or black-list), user credentials (if required) and other sensitive information. Thus, it is necessary to ensure that any device profile containing sensitive information is obtained via an authenticated source, with integrity protection, and delivered to an authenticated device. For sensitive information such as credentials, privacy is also required. The framework requires that devices obtain sensitive information only from authenticated entities except while it is being bootstrapped. In cases where privacy needs to be mandated for notifications, the device provider can configure the device with a SIPS URI, to be used as the subscription URI, during profile enrolment. The framework also requires a PDS presenting sensitive profile data to use digest authentication. This ensures that the data is delivered to an authenticated entity. Authentication of profile retrieval via content indirection for sensitive profiles is via HTTPS utilizing HTTP digest.

E.9.3 User profile

Devices can only request user profiles for users that are known by a SIP service provider. PDSs are required to reject user profile enrolment requests for any users that are unknown in the network. For known user AoRs that are allowed to retrieve profiles, the security considerations are similar to that of the device profile (except for bootstrapping)

Appendix A

PSTN Interconnect for IPCablecom

(This appendix does not form an integral part of this Recommendation)

IPCablecom places requirements on the PSTN interconnect function that are not supported by the Media Gateway Control Function (MGCF), and the Media Gateway (MGW) as specified in 3GPP IMS. For example, an IPCablecom network must support the following services:

– busy line verify and emergency interrupt;

– operator services (e.g., 0+ dialling);

– emergency calling (e.g., 121, 911);

– electronic surveillance;

– local number portability.

Also, IPCablecom requires support of codecs that are not supported by the 3GPP IMS MGW.

These services and capabilities are supported by the IPCablecom media gateway controller (MGC) and media gateway (MG) components. Therefore, IPCablecom replaces the 3GPP MGCF and MGW PSTN interconnect components with the MGC and MG.

Bibliography

[b-IETF RFC 959]	IETF RFC 959 (1985), *File Transfer Protocol*.
[b-IETF RFC 2132]	IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions*".
[b-IETF RFC 4510]	IETF RFC 4510 (2006), *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*.
[b-IETF RFC 4825]	IETF RFC 4825 (2007), *The Extensible Markup Language (XML) Configuration Access Protocol (XCAP).*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2011