

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



International
Telecommunication
Union
Documents

Document Sharing Hub

Downloaded from: 192.168.1.100

Recommendation ITU-T J.366.4

IPCorecom2 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/>.

© ITU 2011

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

	Page
1 Scope	1
2 References.....	1
3 Definitions	1
3.1 Terms defined elsewhere	1
3.2 Terms defined in this Recommendation.....	1
4 Abbreviations and acronyms	1
5 Conventions	1
6 Modifications to [ETSI TS 124 229]	2
Appendix A – PSTN Interconnect for IPCablecom.....	120
Bibliography.....	121

.....

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: "IP-Cablecom 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 IP-Cablecom 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 IP-Cablecom architecture defines a set of reference points to allow a cable IP-CAN to utilize an IMS core. Included in the IP-Cablecom architecture is a reference point, PKT-QOS-1 \(see the IP-Cablecom Quality of Service Overview \[82\], and the IP-Cablecom 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, the UE and the P-CSCF shall send and receive request and responses other than an initial REGISTER requests on the protected ports as described in 3GPP TS 33.203 [ITU-T J.366.7] [1998].

...

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] [1998].

...

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](#)The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the protected port value see ~~3GPP TS 33.203~~ [ITU-T J.366.7 \[4998\]](#).

[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~~The UE shall support the setup of two pairs of security associations as defined in ~~3GPP TS 33.203~~ [ITU-T J.366.7 \[4998\]](#). 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 \[4998\]](#). 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 [1998], 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~~The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 ITU-T J.366.7 [1998].

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 [1998] 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~~
- ~~e) 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[1998] 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[1998]), 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[1998];
- 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~~hen 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~~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 ~~identity~~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 [~~1998~~]);
- 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 ~~subclause~~[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 ~~subclause~~[subclause](#) 5.1.1.2; and
 - b) by performing a subscription to the reg event package as described in ~~subclause~~[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 upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element\(s\) which were registered by this UE with:](#)

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

the UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the initial registration procedure as described in subclause 5.1.1.2. 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,](#) ~~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~~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~~The~~ UE shall discard any SIP request that is not integrity protected and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

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

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

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](#)The 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 stream.](#)

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~~The P-CSCF will integrity protect all SIP messages sent to the UE outside of the registration and authentication procedures. The P-CSCF will discard any SIP message that is not ~~integrity~~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~~When~~ 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 [1998]. 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 [1998] 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 [1998].

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

- 1) reduce the SIP level lifetime of the old set of security associations towards the same UE to $64 \cdot T1$ (if currently longer than $64 \cdot T1$); and
- 2) use the newly established set of security associations for further messages sent towards the UE as appropriate (i.e., take the newly established set of security associations into use).

NOTE 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 ~~shorter~~shorter than $64 \cdot T1$ and a newly established set of security associations has not been taken into use, the P-CSCF shall use the newly ~~established~~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) ~~response~~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 routing 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 $64 \cdot T1$, if lifetime is larger than $64 \cdot T1$
SIP message received over old set of security associations	No action	No action	No action
Old set of security associations currently in use will expire in $64 \cdot T1$	No action	Take into use	No action

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 ~~UEs~~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-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