

Source: TSG CN WG1
Title: CR on Rel-6 WI IMS2 towards TS 24.229
Agenda item: 9.1
Document for: APPROVAL

This document contains **1 CR on Rel-6 Work Item “IMS2”** on “Ipv6 IPv4 interworking”. The CR has been agreed by TSG CN WG1 CN#35 meeting and forwarded to TSG CN Plenary meeting #25 for approval.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	Current version	WI	Rel
N1-041630	Ipv6 IPv4 interworking	24.229	692	2	B	6.3.0	IMS2	Rel-6

CR-Form-v7

CHANGE REQUEST

☼ **24.229 CR 692** ☼ rev **2** ☼ Current version: **6.3.0** ☼

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ☼ symbols.

Proposed change affects: UICC apps☼ ME Radio Access Network Core Network

Title:	☼	IPv6 IPv4 interworking	
Source:	☼	Ericsson	
Work item code:	☼	IMS2	Date: ☼ 10/08/2004
Category:	☼	B	Release: ☼ Rel-6
		Use <u>one</u> of the following categories: F (correction) A (corresponds to a correction in an earlier release) B (addition of feature), C (functional modification of feature) D (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900 .	Use <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) Rel-4 (Release 4) Rel-5 (Release 5) Rel-6 (Release 6)

Reason for change:	☼	TS 23.228 defines how interworking towards IPv4 networks shall be done. The stage 3 work of it is missing from TS24.229.
Summary of change:	☼	A reference to TS 29.262 is added. The abbreviation IMS-ALG is added. The procedures to be followed by the S-CSCF is added. IMS-ALG is added in 4.1. Two new sections 5.9 and 6.7 are added which define the IMS-ALG
Consequences if not approved:	☼	The communication towards IPv4 networks will not be possible.

Clauses affected:	☼	2, 3, 4.1, 5.4.3.2, 5.7, 6.7				
Other specs affected:	☼	<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="width: 20px; text-align: center;">Y</td> <td style="width: 20px; text-align: center;">N</td> </tr> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Other core specifications ☼	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Y	N					
<input type="checkbox"/>	<input checked="" type="checkbox"/>					
		<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> Test specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/>					
		<table border="1" style="display: inline-table; border-collapse: collapse;"> <tr> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input checked="" type="checkbox"/></td> </tr> </table> O&M Specifications	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	<input checked="" type="checkbox"/>					
Other comments:	☼					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at <http://www.3gpp.org/specs/CR.htm>. Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ☼ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/>. For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

First changed section

2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [2] 3GPP TS 23.002: "Network architecture".
- [3] 3GPP TS 23.003: "Numbering, addressing and identification".
- [4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".
- [4A] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".
- [5] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".
- [6] 3GPP TS 23.221: "Architectural requirements".
- [7] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".
- [8] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".
- [8A] 3GPP TS 24.141: "Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".
- [8B] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".
- [9] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".
- [9A] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".
- [10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".
- [10A] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services".
- [11] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".
- [12] 3GPP TS 29.207: "Policy control over Go interface".
- [13] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".
- [13A] 3GPP TS 29.209: "Policy control over Gq interface".
- [14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".
- [15] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".

- [16] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".
- [17] 3GPP TS 32.260: "Telecommunication management; Charging management; IP Multimedia Subsystem (IMS) charging".
- [18] 3GPP TS 33.102: "3G Security; Security architecture".
- [19] 3GPP TS 33.203: "Access security for IP based services".
- [19A] 3GPP TS 33.210: "IP Network Layer Security".
- [20] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".
- [20A] RFC 2401 (November 1998): "Security Architecture for the Internet Protocol".
- [20B] RFC 1594 (March 1994): "FYI on Questions and Answers to Commonly asked "New Internet User" Questions".
- [20C] RFC 2403 (November 1998) "The Use of HMAC-MD5-96 within ESP and AH".
- [20D] RFC 2404 (November 1998) "The Use of HMAC-SHA-1-96 within ESP and AH".
- [20E] RFC 2462 (November 1998): "IPv6 Address Autoconfiguration".
- [21] RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication".
- [22] RFC 2806 (April 2000): "URLs for Telephone Calls".
- [23] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".
- [24] RFC 2916 (September 2000): "E.164 number and DNS".
- [25] RFC 2976 (October 2000): "The SIP INFO method".
- [25A] RFC 3041 (January 2001): "Privacy Extensions for Stateless Address Autoconfiguration in IPv6".
- [26] RFC 3261 (June 2002): "SIP: Session Initiation Protocol".
- [27] RFC 3262 (June 2002): "Reliability of provisional responses in Session Initiation Protocol (SIP)".
- [28] RFC 3265 (June 2002): "Session Initiation Protocol (SIP) Specific Event Notification".
- [29] RFC 3311 (September 2002): "The Session Initiation Protocol (SIP) UPDATE method".
- [30] RFC 3312 (October 2002): "Integration of resource management and Session Initiation Protocol (SIP)".
- [31] RFC 3313 (January 2003): "Private Session Initiation Protocol (SIP) Extensions for Media Authorization".
- [32] RFC 3320 (March 2002): "Signaling Compression (SigComp)".
- [33] RFC 3323 (November 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".
- [34] RFC 3325 (November 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".
- [34A] RFC 3326 (December 2002): "The Reason Header Field for the Session Initiation Protocol (SIP)".
- [35] RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".
- [36] RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) REFER method".
- [37] RFC 3420 (November 2002): "Internet Media Type message/sipfrag".

[38] RFC 3608 (October 2003): "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration".

[39] draft-ietf-mmusic-sdp-new-13 (May 2003): "SDP: Session Description Protocol".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

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

[41] RFC 3319 (July 2003): "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[42] RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) static dictionary for Signaling Compression (SigComp)".

[43] RFC 3680 (March 2004): "A Session Initiation Protocol (SIP) Event Package for Registrations".

[44] Void.

[45] Void.

[46] Void.

[47] Void.

[48] RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[49] RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[51] Void.

[52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)".

[53] RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol".

[54] RFC 3524 (April 2003): "Mapping of Media Streams to Resource Reservation Flows".

[55] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)".

[56] RFC 3556 (July 2003): "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[56A] RFC 3581 (August 2003): "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".

[56B] draft-ietf-sip-callerprefs-10 (October 2003): "Caller Preferences for the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[57] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[58] draft-ietf-sip-session-timer-13 (January 2004): "Session Timers in the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[70] draft-ietf-sip-publish-02 (January 2004): "Session Initiation Protocol (SIP) Extension for Presence Publication".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[71] draft-niemi-sipping-event-throttle-00 (October 2003): "Session Initiation Protocol (SIP) Event Notification Throttles".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[72] draft-ietf-simple-winfo-package-05 (January 2003): "A Session Initiation Protocol (SIP) Event Template-Package for Watcher Information".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[74] draft-ietf-simple-presence-10 (January 2003): "A Presence Event Package for the Session Initiation Protocol (SIP)".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[75] draft-ietf-simple-event-list-04 (June 2003): "A Session Initiation Protocol (SIP) Event Notification Extension for Collections".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[77] draft-ietf-simple-xcap-package-01 (February 2004): "A Session Initiation Protocol (SIP) Event Package for Modification Events for the Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Managed Documents".

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

[78] draft-ietf-sipping-conference-package-03 (February 2004): "A Session Initiation Protocol (SIP) Event Package for Conference State"

[78] [TS 29.162 Interworking between the IM CN subsystem and IP networks](#)

Next changed section

3 Definitions and abbreviations

3.1 Definitions

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

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

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

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

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

Fully-Qualified Domain Name (FQDN)

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

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

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

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

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

Filter criteria
Initial filter criteria
Initial request
Standalone transaction
Subsequent request

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

Interrogating-CSCF (I-CSCF)
IP-Connectivity Access Network (IP-CAN)
Policy Decision Function (PDF)
Private user identity
Proxy-CSCF (P-CSCF)
Public user identity
Serving-CSCF (S-CSCF)

[IMS Application Level Gateway \(IMS-ALG\)](#)

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

IM Subscriber Identity Module (ISIM)
Protected server port

Protected client port

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

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

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

Security association

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

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

International public telecommunication number

3.2 Abbreviations

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

1xx	A status-code in the range 101 through 199, and excluding 100
2xx	A status-code in the range 200 through 299
AS	Application Server
APN	Access Point Name
AUTN	Authentication Token
B2BUA	Back-to-Back User Agent
BGCF	Breakout Gateway Control Function
c	conditional
CCF	Charging Collection Function
CDR	Charging Data Record
CK	Ciphering Key
CN	Core Network
CSCF	Call Session Control Function
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTD	Document Type Definition
ECF	Event Charging Function
FQDN	Fully Qualified Domain Name
GCID	GPRS Charging Identifier
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
HSS	Home Subscriber Server
i	irrelevant
I-CSCF	Interrogating CSCF
ICID	IM CN subsystem Charging Identifier
IK	Integrity Key
IM	IP Multimedia
IMS	IP Multimedia core network Subsystem
IMSI	International Mobile Subscriber Identity
IMS-ALG	IMS Application Level Gateway
IOI	Inter Operator Identifier
IP	Internet Protocol
IP-CAN	IP-Connectivity Access Network
IPsec	IP security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISC	IP multimedia Subsystem Service Control

ISIM	IM Subscriber Identity Module
m	mandatory
MAC	Message Authentication Code
MCC	Mobile Country Code
MGCF	Media Gateway Control Function
MGW	Media Gateway
MNC	Mobile Network Code
MRFC	Multimedia Resource Function Controller
MRFP	Multimedia Resource Function Processor
PDP	Packet Data Protocol
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
n/a	not applicable
NAI	Network Access Identifier
o	optional
P-CSCF	Proxy CSCF
PDU	Protocol Data Unit
RAND	RANDom challenge
RES	RESponse
RTCP	Real-time Transport Control Protocol
RTP	Real-time Transport Protocol
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SQN	SeQuence Number
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Universal Resource Identifier
URL	Universal Resource Locator
USIM	Universal Subscriber Identity Module
x	prohibited
XMAC	expected MAC
XML	eXtensible Markup Language

Next changed section

4 General

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

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

Each IM CN subsystem functional entity using an interface at the Gm reference point, the Mg reference point, the Mi reference point, the Mj reference point, the Mk reference point, the Mm reference point, the Mr reference point and the Mw reference point, and also using the IP multimedia Subsystem Service Control (ISC) Interface, shall implement SIP, as defined by the referenced specifications in Annex A, and in accordance with the constraints and provisions specified in annex A, according to the following roles.

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

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

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

- The User Equipment (UE) shall provide the User Agent (UA) role, with the exceptions and additional capabilities to SIP as described in subclause 5.1, with the exceptions and additional capabilities to SDP as described in subclause 6.1, and with the exceptions and additional capabilities to SigComp as described in subclause 8.1. The UE shall also provide the access dependent procedures described in subclause B.2.2.
- The P-CSCF shall provide the proxy role, with the exceptions and additional capabilities to SIP as described in subclause 5.2, with the exceptions and additional capabilities to SDP as described in subclause 6.2, and with the exceptions and additional capabilities to SigComp as described in subclause 8.2. Under certain circumstances as described in subclause 5.2, the P-CSCF shall provide the UA role with the additional capabilities, as follows:
 - a) when acting as a subscriber to or the recipient of event information; and
 - b) when performing P-CSCF initiated dialog-release the P-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.
- The I-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.3.
- The S-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.4, and with the exceptions and additional capabilities to SDP as described in subclause 6.3. Under certain circumstances as described in subclause 5.4, the S-CSCF shall provide the UA role with the additional capabilities, as follows:
 - a) the S-CSCF shall also act as a registrar. When acting as a registrar, or for the purposes of executing a third-party registration, the S-CSCF shall provide the UA role;
 - b) as the notifier of event information the S-CSCF shall provide the UA role;
 - c) when providing a messaging mechanism by sending the MESSAGE method, the S-CSCF shall provide the UA role; and
 - d) when performing S-CSCF initiated dialog release the S-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.
- The MGCF shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.5, and with the exceptions and additional capabilities to SDP as described in subclause 6.4.
- The BGCF shall provided the proxy role, with the exceptions and additional capabilities as described in subclause 5.6.
- The AS, acting as terminating UA, or redirect server (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.1), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.2, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.
- The AS, acting as originating UA (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.2), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.3, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.
- The AS, acting as a SIP proxy (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.3), shall provided the proxy role, with the exceptions and additional capabilities as described in subclause 5.7.4.
- The AS, performing 3rd party call control (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.4), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.5, and with the exceptions and additional capabilities to SDP as described in subclause 6.6.

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

- The AS, receiving third-party registration requests, shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.
- The MRFC shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.8, and with the exceptions and additional capabilities to SDP as described in subclause 6.5.

NOTE 2: Annex A can change the status of requirements in referenced specifications. Particular attention is drawn to table A.4 and table A.162 for capabilities within referenced SIP specifications, and to table A.317 and table A.328 for capabilities within referenced SDP specifications. The remaining tables build on these initial tables.

NOTE 3: The allocated roles defined in this clause are the starting point of the requirements from the IETF SIP specifications, and are then the basis for the description of further requirements. Some of these extra requirements formally change the proxy role into a B2BUA. In all other respects other than those more completely described in subclause 5.2a P-CSCF implements proxy requirements. Despite being a B2BUA a P-CSCF does not implement UA requirements from the IETF RFCs, except as indicated in this specification, e.g., relating to registration event subscription.

- [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.](#)

Next changed section

5.4.3.2 Requests initiated by the served user

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

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

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

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

- 2) remove its own SIP URI from the topmost Route header;
- 3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request;
- 4) check whether the initial request matches the initial filter criteria based on a public user identity in the P-Asserted-Identity header, and if it does, forward this request to that AS, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted AS as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous process, the S-CSCF may contact one or more AS(s) before processing the outgoing Request-URI. In case of contacting one or more AS(s) the S-CSCF shall:
 - a) insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4; and
 - b) if the AS is located outside the trust domain then the S-CSCF shall remove the P-Access-Network-Info header field and its values in the request; if the AS is located within the trust domain, then the S-CSCF shall retain the P-Access-Network-Info header field and its values in the request that is forwarded to the AS;

- 5) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. Optionally, the S-CSCF may generate a new, globally unique icid and insert the new value in the icid parameter of the P-Charging-Vector header when forwarding the message. If the S-CSCF creates a new icid, then it is responsible for maintaining the two icid values in the subsequent messaging;
- 6) insert an orig-ioi parameter into the P-Charging-Vector header. The S-CSCF shall set the orig-ioi parameter to a value that identifies the sending network. The S-CSCF shall not include the term-ioi parameter;
- 7) insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;
- 8) in the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URI contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;
- 9) if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [22]) to a globally routeable SIP URI using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator;
- 10) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header if present, otherwise based on the Request-URI. If the destination address is of an IP address -type- other than the IP address type used in the IM CN subsystem , then the S-CSCF shall forward the request to the IMS-ALG if the IM CN subsystem supports interworking to networks with different IP address type;
- 11) if network hiding is needed due to local policy, put the address of the I-CSCF(THIG) to the topmost route header;
- 12) in case of an initial request for a dialog originated from a served user, create a Record-Route header containing its own SIP URI;

NOTE 2: For requests originated from a PSI the S-CSCF can decide whether to record-route or not.

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

- 13) remove the P-Access-Network-Info header prior to forwarding the message based on the destination user (Request-URI);
- 14) route the request based on SIP routing procedures; and
- 15) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed.

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

- 1) apply any privacy required by RFC 3323 [33] to the P-Asserted-Identity header.

NOTE 3: This header would normally only be expected in 1xx or 2xx responses.

NOTE 4: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3323 [33].

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

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

- 1) remove its own URI from the topmost Route header;
- 2) create a Record-Route header containing its own SIP URI;

- 3) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;
- 4) in case the request is routed towards the destination user (Request-URI) or is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header; and
- 5) route the request based on the topmost Route header.

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

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

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

Last change

[5.9 IMS-ALG](#)

[5.9.1 General](#)

[The IMS-ALG acts as a B2BUA. The IMS-ALG will internally map the message headers between the two dialogs that it manages. It is responsible for correlating the dialog identifiers and will decide when to simply translate a message from one dialog to the other, or when to perform other functions. The IMS-ALG, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem.](#)

[The internal function of the IMS -ALG is defined in 3GPP TS 29.162 \[33\].](#)

[6.7 Procedures at the IMS-ALG](#)

[IMS-ALG makes procedures as for an originating UA and terminating UA. The IMS-ALG acts as a B2BUA. The treatment of the SDP information between originating UA and terminating UA is described in 3GPP TS 29.162 \[33\].](#)

End of changes
