

**Source:** TSG CN WG 1  
**Title:** CRs to Rel-6 on Work Item IMS2 towards 24.229  
**Agenda item:** 9.1  
**Document for:** APPROVAL

---

**Introduction:**

This document contains 7 CRs, **Rel-6** Work Item "IMS2", that have been agreed by **TSG CN WG1** in **CN1#32 meeting**, and are forwarded to TSG CN Plenary meeting #22 for approval.

<b>TDoc #</b>	<b>Tdoc Title</b>	<b>Spec</b>	<b>CR #</b>	<b>Rev</b>	<b>CAT</b>	<b>C_Version</b>	<b>Rel</b>
N1-031469	Corrections on charging specification number	24.229	529		F	6.0.0	Rel-6
N1-031622	IMS trust domain in Rel 6	24.229	551	1	C	6.0.0	Rel-6
N1-031727	SDP offer handling in SIP responses in S-CSCF and P-CSCF	24.229	560	2	B	6.0.0	Rel-6
N1-031705	SIP compression	24.229	564	1	F	6.0.0	Rel-6
N1-031589	Text harmonisation with 3GPP2	24.229	572		D	6.0.0	Rel-6
N1-031680	Procedures in the absence of UICC	24.229	573	1	B	6.0.0	Rel-6
N1-031683	P-Access-Network-Info changes	24.229	575	1	D	6.0.0	Rel-6

CR-Form-v7

## CHANGE REQUEST

⌘ **24.229 CR 529** ⌘ rev **-** ⌘ Current version: **6.0.0** ⌘

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

<b>Title:</b>	⌘ Corrections on charging specification number		
<b>Source:</b>	⌘ NEC Corporation		
<b>Work item code:</b>	⌘ IMS2	<b>Date:</b>	⌘ 18/10/2003
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ Rel-6
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> of the following releases: <b>2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>Rel-4</b> (Release 4) <b>Rel-5</b> (Release 5) <b>Rel-6</b> (Release 6)

<b>Reason for change:</b>	⌘ The charging specifications for rel6 are restructured, taken into account the emerging services for rel6 onwards. 24.229 needs to be aligned accordingly..		
<b>Summary of change:</b>	⌘ Stage2 IMS related charging specification number is changed from TS32.200 to TS32.240.  Stage3 IMS charging specification number is changed from TS32.225 to TS32.260.		
<b>Consequences if not approved:</b>	⌘ Inconsistency is remained between 24.229 and charging specifications.		

<b>Clauses affected:</b>	⌘ 2, 4.5.1, 4.5.2						
<b>Other specs affected:</b>	<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="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> Test 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="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> O&M Specifications	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	⌘	
Y	N						
<input type="checkbox"/>	<input checked="" type="checkbox"/>						
<b>Other comments:</b>	⌘						

**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.

## Start of first change

---

## 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".
- [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 Gs interface".
- [13] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".
- [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.~~200~~240: "Telecommunication management; [Charging management](#); [Charging architecture and principles](#) ~~Charging management; Charging principles~~".
- [17] 3GPP TS 32.~~225~~260: "Telecommunication management; [Charging management](#); [IP Multimedia Subsystem \(IMS\) charging](#) ~~Charging management; Charging data description for the IP Multimedia subsystem~~".

- [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".
- [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] draft-ietf-sip-scvrtdisco-04 (May 2003): "Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration".

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

- [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] draft-ietf-sipping-reg-event-00 (October 2002): "A Session Initiation Protocol (SIP) Event Package for Registrations".

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

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

**End of first change**

**Start of second change**

## 4.5.1 Overview

This subclause describes charging correlation principles to aid with the readability of charging related procedures in clause 5. See 3GPP TS 32.200-240 [16] and 3GPP TS 32.225-260 [17] for further information on charging.

The IM CN subsystem generates and retrieves the following charging correlation information for later use with offline and online charging:

1. IM CN subsystem Charging Identifier (ICID);
2. Access network charging information:
  - a. GPRS Charging Information;

3. Inter Operator Identifier (IOI);
4. Charging function addresses:
  - a. Charging Collection Function (CCF);
  - b. Event Charging Function (ECF).

How to use and where to generate the parameters in IM CN subsystems are described further in the subclauses that follow. The charging correlation information is encoded in the P-Charging-Vector header as defined in subclause 7.2A.5. The P-Charging-Vector header contains the following parameters: icid, access network charging information and ioi.

The offline and online charging function addresses are encoded in the P-Charging-Function-Addresses as defined in RFC 3455 [52]. The P-Charging-Function-Addresses header contains the following parameters: CCF and ECF.

## 4.5.2 IM CN subsystem charging identifier (ICID)

The ICID is the session level data shared among the IM CN subsystem entities including ASs in both the calling and called IM CN subsystems.

The first IM CN subsystem entity involved in a dialog (session) or standalone (non-session) method will generate the ICID and include it in the icid parameter of the P-Charging-Vector header in the SIP request. See 3GPP TS 32.225-260 [17] for requirements on the format of ICID. The P-CSCF will generate an ICID for mobile-originated calls. The I-CSCF will generate an ICID for mobile-terminated calls if there is no ICID received in the initial request (e.g. the calling party network does not behave as an IM CN subsystem). The AS will generate an ICID when acting as an originating UA. The MGCF will generate an ICID for PSTN/PLMN originated calls. Each entity that processes the SIP request will extract the ICID for possible later use in a CDR. The I-CSCF and S-CSCF are also allowed to generate a new ICID for mobile terminated calls received from another network.

There is also an ICID generated by the P-CSCF with a REGISTER request that is passed in a unique instance of P-Charging-Vector header. This ICID is valid for the duration of the registration and is associated with the signalling PDP context.

The icid parameter is included in any requests that include the P-Charging-Vector header. However, the P-Charging-Vector (and ICID) is not passed to the UE.

The ICID is also passed from the P-CSCF to the GGSN via PDF, but the ICID is not passed to the SGSN. The interface supporting this operation is outside the scope of this document.

**End of second change**

Bangkok, Thailand, 27 – 31 October 2003

CR-Form-v7

**CHANGE REQUEST**⌘ **24.229** **CR** **551** ⌘ rev **1** ⌘ Current version: **6.0.0** ⌘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 

<b>Title:</b>	⌘ IMS trust domain in Rel 6		
<b>Source:</b>	⌘ Ericsson		
<b>Work item code:</b>	⌘ IMS2	<b>Date:</b>	⌘ 27/10/2003
<b>Category:</b>	⌘ <b>C</b>	<b>Release:</b>	⌘ Rel-6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	<b>F</b> (correction)		2 (GSM Phase 2)
	<b>A</b> (corresponds to a correction in an earlier release)		R96 (Release 1996)
	<b>B</b> (addition of feature),		R97 (Release 1997)
	<b>C</b> (functional modification of feature)		R98 (Release 1998)
	<b>D</b> (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

<b>Reason for change:</b>	⌘ The concept of the IMS trust domain has been recently discussed in a joint SA3-CN1 session. This CR clarifies that Release 6, IMS is an open network and traffic may be received from either trusted or not trusted nodes. Similarly, SIP traffic can be sent to trusted and non-trusted nodes.
<b>Summary of change:</b>	⌘ This CR provides the IMS nodes with the existence of a mechanism to identify whether the previous/next hop is part of the IMS domain or not. The exact detailed mechanism is left FFS pending of a similar discussion in SA2 and SA3.
<b>Consequences if not approved:</b>	⌘ IMS nodes will not be able to take an appropriate action on the P-Asserted-Identity.

<b>Clauses affected:</b>	⌘ 4.4										
<b>Other specs affected:</b>	⌘	<table border="1"> <tr> <td>Y</td> <td>N</td> </tr> <tr> <td></td> <td>X</td> </tr> <tr> <td></td> <td>X</td> </tr> <tr> <td></td> <td>X</td> </tr> </table>	Y	N		X		X		X	Other core specifications ⌘ Test specifications ⌘ O&M Specifications ⌘
Y	N										
	X										
	X										
	X										
<b>Other comments:</b>	⌘										



## 4.4 Trust domain

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

[Editor's Note: the exact mechanism to determine which nodes are part of the trust domain and which nodes are not, is FFS.](#)

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

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

CR-Form-v7

## CHANGE REQUEST

# 24.229 CR 560 # rev 2- # Current version: 6.0.0 #

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

<b>Title:</b>	# SDP offer handling in SIP responses in S-CSCF and P-CSCF		
<b>Source:</b>	# Nokia		
<b>Work item code:</b>	# IMS2	<b>Date:</b>	# 18/10/2003
<b>Category:</b>	# <b>B</b>	<b>Release:</b>	# Rel-6
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	<b>F</b> (correction)		2 (GSM Phase 2)
	<b>A</b> (corresponds to a correction in an earlier release)		R96 (Release 1996)
	<b>B</b> (addition of feature),		R97 (Release 1997)
	<b>C</b> (functional modification of feature)		R98 (Release 1998)
	<b>D</b> (editorial modification)		R99 (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Rel-4 (Release 4)
			Rel-5 (Release 5)
			Rel-6 (Release 6)

<b>Reason for change:</b>	# SDP offer is allowed in SIP responses in Rel-6. Its handling is not described in the specification.
<b>Summary of change:</b>	# The P-CSCF and S-CSCF related subchapters of "Application usage of SDP" is extended.
<b>Consequences if not approved:</b>	# SDP offer handling in SIP responses is not clarified for P-CSCF and S-CSCF.

<b>Clauses affected:</b>	# 6.2, 6.3										
<b>Other specs affected:</b>	<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;">X</td> <td style="text-align: center;"></td> </tr> <tr> <td style="text-align: center;"></td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;"></td> <td style="text-align: center;">X</td> </tr> </table>	Y	N	X			X		X	Other core specifications	# 29.208
Y	N										
X											
	X										
	X										
		Test specifications									
		O&M Specifications									
<b>Other comments:</b>	#										

### 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.

## 6.2 Procedures at the P-CSCF

When the P-CSCF receives any SIP request containing [an SDP offer](#), the P-CSCF shall examine the media parameters in the received SDP. If the P-CSCF finds any media parameters which are not allowed on the network by local policy, the P-CSCF shall return a 488 (Not Acceptable Here) response containing SDP payload. This SDP payload contains either all the media types, codecs and other SDP parameters which are allowed according to the local policy, or, based on configuration by the operator of the P-CSCF, a subset of these allowed parameters. This subset may depend on the content of the received SIP request. The P-CSCF shall build the SDP payload in the 488 (Not Acceptable Here) response in the same manner as a UAS builds the SDP in a 488 (Not Acceptable Here) response as specified in RFC 3261 [26]. The P-CSCF shall order the SDP payload with the most preferred codec listed first.

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

When the P-CSCF receives an initial INVITE request for a terminating session setup or a 183 (Session Progress) response to an INVITE request for an originating session setup, the P-CSCF may modify the SDP according to RFC 3524 [54] to indicate to the UE that particular media stream(s) is grouped according to a local policy. The policy is used to determine whether the P-CSCF will request the UE to keep media stream(s) grouped in different PDP contexts and identify the relation between different media streams and PDP contexts (see subclause 9.2.5).

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

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

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

## 6.3 Procedures at the S-CSCF

When the S-CSCF receives any SIP request containing [an SDP offer](#), the S-CSCF shall examine the media parameters in the received SDP. If the S-CSCF finds any media parameters which are not allowed based on either local policy or the subscription, the S-CSCF shall return a 488 (Not Acceptable Here) response containing SDP payload. This SDP payload contains either all the media types, codecs and other SDP parameters which are allowed according to the local policy and users subscription or, based on configuration by the operator of the S-CSCF, a subset of these allowed parameters. This subset may depend on the content of the received SIP request. The S-CSCF shall build the SDP payload in the 488 (Not Acceptable Here) response in the same manner as a UAS builds the SDP in a 488 (Not Acceptable Here) response as specified in RFC 3261 [26].

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

CR-Form-v7

## CHANGE REQUEST

# 24.229 CR 564 # rev 1- # Current version: 6.0.0 #

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

<b>Title:</b>	# SIP compression				
<b>Source:</b>	# Nokia				
<b>Work item code:</b>	# IMS2-CGR	<b>Date:</b>	# 18/10/2003		
<b>Category:</b>	# <span style="border: 1px solid black; padding: 2px;">E A</span>	<b>Release:</b>	# Rel-6		
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:		
	<b>F</b> (correction)		2 (GSM Phase 2)		
	<b>A</b> (corresponds to a correction in an earlier release)		R96 (Release 1996)		
	<b>B</b> (addition of feature),		R97 (Release 1997)		
	<b>C</b> (functional modification of feature)		R98 (Release 1998)		
	<b>D</b> (editorial modification)		R99 (Release 1999)		
	Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Rel-4 (Release 4)		
			Rel-5 (Release 5)		
			Rel-6 (Release 6)		

<b>Reason for change:</b>	# It clarifies that the UE may send even the first message compressed.
<b>Summary of change:</b>	# A note has been added.
<b>Consequences if not approved:</b>	# Might lead to problems if the P-CSCF does not save state and the UE has no ways to find this out.

<b>Clauses affected:</b>	# 8.1.2								
<b>Other specs affected:</b>	<table style="display: inline-table; border-collapse: collapse;"> <tr> <td style="border: 1px solid black; padding: 2px;">Y</td> <td style="border: 1px solid black; padding: 2px;">N</td> </tr> <tr> <td style="border: 1px solid black; padding: 2px;">#</td> <td style="border: 1px solid black; padding: 2px;">X</td> </tr> <tr> <td style="border: 1px solid black; padding: 2px;">#</td> <td style="border: 1px solid black; padding: 2px;">X</td> </tr> <tr> <td style="border: 1px solid black; padding: 2px;">#</td> <td style="border: 1px solid black; padding: 2px;">X</td> </tr> </table> Other core specifications # Test specifications # O&M Specifications #	Y	N	#	X	#	X	#	X
Y	N								
#	X								
#	X								
#	X								
<b>Other comments:</b>	#								

### 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.

---

## 8 SIP compression

### 8.1 SIP compression procedures at the UE

#### 8.1.1 SIP compression

The UE shall support SigComp as specified in RFC 3320 [32]. When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486 [55]. The compartment shall finish when the UE is no longer registered. State creations and announcements shall be allowed only for messages received in a security association.

The UE shall support the SIP dictionary specified in RFC 3485 [42]. If compression is enabled, the UE shall use the dictionary to compress the first message.

#### 8.1.2 Compression of SIP requests and responses transmitted to the P-CSCF

The UE should compress the requests and responses transmitted to the P-CSCF according to subclause 8.1.1.

NOTE1: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

NOTE2: [Since compression support is mandatory, the UE may send even the first message compressed. Sigcomp provides mechanisms to allow the UE to know if state has been created in the P-CSCF or not.](#)

#### 8.1.3 Decompression of SIP requests and responses received from the P-CSCF

The UE shall decompress the compressed requests and responses received from the P-CSCF according to subclause 8.1.1.

If the UE detects a decompression failure at the P-CSCF, the recovery mechanism is implementation specific and this may, as an example, include resetting the compartment, changing the algorithm or sending the following message(s) without compression.

### 8.2 SIP compression procedures at the P-CSCF

#### 8.2.1 SIP compression

The P-CSCF shall support SigComp as specified in RFC 3320 [32]. When using SigComp the P-CSCF shall send compressed SIP messages in accordance with RFC 3486 [55]. The compartment shall finish when the UE is no longer registered. State creations and announcements shall be allowed only for messages received in a security association.

The P-CSCF shall support the SIP dictionary specified in RFC 3485 [42]. If compression is enabled, the P-CSCF shall use the dictionary to compress the first message.

#### 8.2.2 Compression of SIP requests and responses transmitted to the UE

The P-CSCF should compress the requests and responses transmitted to the UE according to subclause 8.2.1.

NOTE: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

### 8.2.3 Decompression of SIP requests and responses received from the UE

The P-CSCF shall decompress the compressed requests and responses received from the UE according to subclause 8.2.1.

If the P-CSCF detects a decompression failure at the UE, the recovery mechanism is implementation specific and this may, as an example, include resetting the compartment, changing the algorithm or sending the following message(s) without compression.



## CHANGE REQUEST

⌘ **24.229 CR 572** ⌘ rev - ⌘ Current version: **6.0.0** ⌘

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

<b>Title:</b>	⌘ Text harmonisation with 3GPP2		
<b>Source:</b>	⌘ Lucent Technologies		
<b>Work item code:</b>	⌘ IMS2	<b>Date:</b>	⌘ 15/10/2003
<b>Category:</b>	⌘ <b>D</b>	<b>Release:</b>	⌘ Rel-6
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		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)

<b>Reason for change:</b>	⌘ A number of textual changes have been made in the 3GPP2 version of 3GPP TS 24.229. In a number of cases, these result in a slight textual improvement, and therefore, in order to promote alignment, it is desirable to make these changes to the 3GPP specification rather than commenting to 3GPP2 to reverse their change. This document identifies some of those changes.
<b>Summary of change:</b>	⌘ <ol style="list-style-type: none"> <li>1. In subclause 5.1.1.5A, the capability so provided can only apply to IPv6 and is identified so throughout the text, but not in the title and the final paragraph. Changing the remaining instances of "IP" to "IPv6" does not make any technical change (it certainly does not allow "IPv4" as that is clearly precluded in text in subclause 4.2), but does align with 3GPP2 where they do have to support both IPv4 and IPv6.</li> <li>2. In subclause 5.1.1.6, the keys are held both by the P-CSCF and the S-CSCF, therefore reference to the P-CSCF is not strictly speaking correct, and a more general reference to the IM CN subsystem is to be preferred.</li> <li>3. In subclause 5.1.1.7, a more complete reference is added to the public user identities being deregistered as well.</li> <li>4. In subclause 5.1.3.1, the word "remaining" is considered to be an improvement on "further" and is substituted.</li> <li>5. In subclause 5.4.1.7, the reference to IMSI is deleted, as here it is only an example of contents, it is 3GPP specific, and the issued is covered in other places in other specifications.</li> <li>6. Subclause 5.7.2, and subclause 5.7.4 are changed to correspond to the change made in subclause 7.6.2.</li> <li>7. In subclause 7.6.2, 7.6.3 and 7.7, the label "3GPP" is deleted in preference for "IM CN subsystem" where this has no impact on the codings. (Any change to the codings would have to be made at release 5 because there would be backward compatibility issues otherwise).</li> </ol>

<b>Consequences if not approved:</b>	⌘											
<b>Clauses affected:</b>	⌘	5.1.1.5A, 5.1.1.6, 5.1.1.7, 5.1.3.1, 5.4.1.7, 7.6.2, 7.6.3, 7.7										
<b>Other specs affected:</b>	⌘	<table border="1"> <tr> <td>Y</td> <td>N</td> </tr> <tr> <td></td> <td>X</td> </tr> <tr> <td></td> <td>X</td> </tr> <tr> <td></td> <td>X</td> </tr> </table>	Y	N		X		X		X	Other core specifications	⌘
		Y	N									
			X									
	X											
	X											
		Test specifications										
		O&M Specifications										
<b>Other comments:</b>	⌘											

**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.

## PROPOSED CHANGE

### 5.1.1.5A Change of IPv6 address due to privacy

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

If the UE receives an IPv6 prefix, the UE may change the interface identity of the IPv6 address as described in RFC 3041 [25A] due to privacy but this will result in service discontinuity for IMS services.

**NOTE:** The procedure described below will terminate all established dialogs and transactions and temporarily disconnect the UE from the IM CN subsystem until the new registration is performed. Due to this, the UE is recommended to provide a limited use of the procedure to ensure a maximum degree of continuous service to the end user.

In order to change the IPv6 address due to privacy, the UE shall:

- 1) terminate all ongoing dialogs (e.g., sessions) and transactions (e.g., subscription to the reg event);
- 2) deregister all registered public user identities as described in subclause 5.1.1.4;
- 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 5.1.1.2; and
  - b) by performing a subscription to the reg event package as described in subclause 5.1.1.3; and
- 5) subscribe to other event packages it was subscribed to before the change of IPv6 address procedure started.

## PROPOSED CHANGE

### 5.1.1.6 Mobile-initiated deregistration

The UE can deregister a previously registered public user identity at any time.

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

The UE shall extract or derive from the UICC 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) the Authorization header, with the username field, set to the value of the private user identity;
- b) the From header set to the SIP URI that contains the public user identity to be deregistered;
- c) the To header set to the SIP URI that contains the public user identity to be deregistered;
- d) the Contact header set to either the value of "\*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and the protected server port value bound to the security association;
- e) the Expires header, or the expires parameter of the Contact header, set to the value of zero, appropriate to the deregistration requirements of the user;

- f) a Request-URI set to the SIP URI of the domain name of the home network; and
- g) a P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

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

If there are no more public user identities registered, the UE shall delete the security associations and related keys it may have towards the ~~P-CSCF~~[IM CN subsystem](#).

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

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

## PROPOSED CHANGE

### 5.1.1.7 Network-initiated deregistration

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) with the state attribute set to "terminated" and the event attribute set to "rejected" or "deactivated", the UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the reregistration procedure as described in subclause 5.1.1.4. 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 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 contains the value of "terminated", the UE shall delete the security associations towards the P-CSCF after the server transaction (as defined in RFC 3261 [26]) pertaining to the NOTIFY request terminates.

NOTE 1: Deleting a security association is an internal procedure of the UE and does not involve any SIP procedures.

NOTE 2: If [all public user identities are deregistered and](#) the security association ~~towards the P-CSCF~~ is removed, then the UE considers the subscription to the reg event package terminated (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero, or a NOTIFY request was received with Subscription-State header containing the value of "terminated").

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

## PROPOSED CHANGE

### 5.1.3.1 Initial INVITE

Upon generating an initial INVITE request, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism;
- indicate the requirement of precondition and specify it using the Require header mechanism.

NOTE: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26]. The UE may 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.

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall not progress any ~~further~~ 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.

If the UA receives a 503 (Service Unavailable) response to an initial INVITE 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.

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

If the UE receives a 420 (Bad Extension) response to an initial INVITE request with "precondition" option-tag in the Unsupported header field, the UE shall abort the session attempt and shall not resend this INVITE request without "precondition" option-tag in the Require header.

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

## PROPOSED CHANGE

### 5.4.1.7 Notification of Application Servers about registration status

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

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

- a) the Request-URI, which shall contain the AS's SIP URI;
- b) the From header, which shall contain the S-CSCF's SIP URI;
- c) the To header, which shall contain either the public user identity as contained in the REGISTER request received from the UE or one of the implicitly registered public user identities, as configured by the operator;
- d) the Contact header, which shall contain the S-CSCF's SIP URI;
- e) for initial registration and user-initiated reregistration (subclause 5.4.1.2), the Expires header, which shall contain the same value that the S-CSCF returned in the 200 (OK) response for the REGISTER request received from the UE;
- f) for user-initiated deregistration (subclause 5.4.1.4) and network-initiated deregistration (subclause 5.4.1.5), the Expires header, which shall contain the value zero;
- g) for initial registration and user-initiated reregistration (subclause 5.4.1.2), a message body, if there is Filter Criteria indicating the need to include HSS provided data for the REGISTER event (e.g. HSS may provide AS specific data to be included in the third-party REGISTER, ~~such as IMSI to be delivered to IMS SF~~). If there is a service information XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [14]), then the S-CSCF shall include it in the message body of the REGISTER request within the <service-info> XML element as described in subclause 7.6. For the messages including the ~~3GPP-IMS-IM CN subsystem~~ XML body, the S-CSCF shall set the value of the Content-Type header to include the MIME type specified in subclause 7.6;

- h) for initial registration, the P-Charging-Vector header, which shall contain the same icid parameter that the S-CSCF received in the original REGISTER request from the UE;
- i) for initial registration, a P-Charging-Function-Addresses header, which shall contain the values received from the HSS if the message is forwarded within the S-CSCF home network.

## PROPOSED CHANGE

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

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

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

An AS acting as redirect server shall propagate any received [3GPP-IM CN subsystem XML](#) message body in the redirected message.

## PROPOSED CHANGE

### 5.7.4 Application Server (AS) acting as a SIP proxy

When the AS acting as a SIP proxy receives a request from the S-CSCF, prior to forwarding the request it shall:

- remove its own URI from the topmost Route header; and
- after executing the required services, route the request based on the topmost Route header.

The AS may modify the SIP requests based on service logic, prior to forwarding the request back to the S-CSCF.

An AS acting as a SIP proxy shall propagate any received [IM CN subsystem XML](#) ~~3GPP~~ message body in the forwarded message.

## PROPOSED CHANGE

### 7.6.2 Document Type Definition

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

**Table 7.7: ~~3GPP~~-IM CN subsystem XML body, version 1 DTD**

```
<?xml version="1.0" ?>
<!-- Draft DTD for the 3GPP-IMS XML body. -->

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

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

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

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

1 >

## PROPOSED CHANGE

### 7.6.3 DTD description

This subclause describes the elements of the ~~3GPP~~ IMS Document Type Definition as defined in table 7.7.

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

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

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

The <alternative-service> element contains a <type> element that indicates the type of alternative service. In the present document, the <type> element contains only the value "emergency".

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

## PROPOSED CHANGE

### 7.7 SIP timers

The timers defined in RFC 3261 [26] need modification in some cases to accommodate the delays introduced by the air interface processing and transmission delays. Table 7.8 shows recommended values for ~~3GPP~~[the IM CN subsystem](#).

Table 7.8 lists in the first column, titled "SIP Timer" the timer names as defined in RFC 3261 [26].

The second column, titled "~~3GPP~~ value to be applied between ~~network~~[IM CN subsystem](#) elements" lists the values recommended for network elements e.g. P-CSCF, S-CSCF, MGCF, when communicating with each other i.e. when no air interface leg is included. These values are identical to those recommended by RFC 3261 [26].

The third column, titled "~~3GPP~~ value to be applied at the UE" lists the values recommended for the UE. These are modified when compared to RFC 3261 [26] to accommodate the air interface delays.

The fourth column, titled "~~3GPP~~ value to be applied at the P-CSCF toward a UE" lists the values recommended for the P-CSCF when an air interface leg is traversed. These are modified when compared to RFC 3261 [26].

The final column reflects the timer meaning as defined in RFC 3261 [26].

Table 7.8: SIP timers

SIP Timer	3GPP value to be applied between network IM CN subsystem elements	3GPP value to be applied at the UE	3GPP value to be applied at the P-CSCF toward a UE	Meaning
T1	500ms default	2s default	2s default	RTT estimate
T2	4s	16s	16s	The maximum retransmit interval for non-INVITE requests and INVITE responses
T4	5s	17s	17s	Maximum duration a message will remain in the network
Timer A	initially T1	initially T1	initially T1	INVITE request retransmit interval, for UDP only
Timer B	64*T1	64*T1	64*T1	INVITE transaction timeout timer
Timer C	> 3min	> 3 min	> 3 min	proxy INVITE transaction timeout
Timer D	> 32s for UDP 0s for TCP/SCTP	>128s 0s for TCP/SCTP	>128s 0s for TCP/SCTP	Wait time for response retransmits
Timer E	initially T1	initially T1	initially T1	non-INVITE request retransmit interval, UDP only
Timer F	64*T1	64*T1	64*T1	non-INVITE transaction timeout timer
Timer G	initially T1	initially T1	initially T1	INVITE response retransmit interval
Timer H	64*T1	64*T1	64*T1	Wait time for ACK receipt.
Timer I	T4 for UDP 0s for TCP/SCTP	T4 for UDP 0s for TCP/SCTP	T4 for UDP 0s for TCP/SCTP	Wait time for ACK retransmits
Timer J	64*T1 for UDP 0s for TCP/SCTP	64*T1 for UDP 0s for TCP/SCTP	64*T1 for UDP 0s for TCP/SCTP	Wait time for non-INVITE request retransmits
Timer K	T4 for UDP 0s for TCP/SCTP	T4 for UDP 0s for TCP/SCTP	T4 for UDP 0s for TCP/SCTP	Wait time for response retransmits



## CHANGE REQUEST

⌘ **24.229 CR 573** ⌘ rev **1** ⌘ Current version: **6.0.0** ⌘

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

<b>Title:</b>	⌘ Procedures in the absence of UICC		
<b>Source:</b>	⌘ Lucent Technologies		
<b>Work item code:</b>	⌘ IMS2	<b>Date:</b>	⌘ 21/10/2003
<b>Category:</b>	⌘ <b>B</b>	<b>Release:</b>	⌘ Rel-6
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> of the following releases: <b>2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>Rel-4</b> (Release 4) <b>Rel-5</b> (Release 5) <b>Rel-6</b> (Release 6)

<b>Reason for change:</b>	⌘ Subclause 5.1.1.1A specifies procedures for the derivation of parameters for use in the authentication request. In 3GPP, these are taken from the UICC (in respect of commonality text, in 3GPP2 they may well be directly configured in the terminal). If therefore the UICC is absent, the parameters cannot be derived, and the authentication should not proceed.
<b>Summary of change:</b>	⌘ Ann extra requirement is added to subclause 5.1.1.1A
<b>Consequences if not approved:</b>	⌘ No specification in this area.

<b>Clauses affected:</b>	⌘ 5.1.1.1A										
<b>Other specs affected:</b>	<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;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> <tr> <td style="text-align: center;">⌘</td> <td style="text-align: center;">X</td> </tr> </table> Other core specifications Test specifications O&M Specifications	Y	N	⌘	X	⌘	X	⌘	X	⌘	
Y	N										
⌘	X										
⌘	X										
⌘	X										
<b>Other comments:</b>	⌘										

### 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.

### 5.1.1.1A Parameters contained in the UICC

If there is an ISIM and a USIM application on a UICC, then the ISIM application shall always be used for IMS authentication, as described in 3GPP TS 33.203 [19].

In case the UE is loaded with a UICC that contains the ISIM application, it will be preconfigured with all the necessary parameters to initiate the registration to the IM CN subsystem. These parameters include:

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

In case the UE is loaded with a UICC that does not contain the ISIM application, the UE shall:

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to.

All these three parameters are derived from the IMSI parameter in the USIM, according to the procedures described in 3GPP TS 23.003 [3]. If the UICC does not contain the ISIM application, the UE shall derive new values every time the UICC is changed, and shall discard existing values if the UICC is removed.

The temporary public user identity is only used in REGISTER requests, i.e. initial registration, re-registration, mobile-initiated deregistration. After a successful registration, the UE will get the associated public user identities, and the UE may use any of them in subsequent non-REGISTER requests.

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

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

## CHANGE REQUEST

⌘ **24.229 CR 575** ⌘ rev **1** ⌘ Current version: **6.0.0** ⌘

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

<b>Title:</b>	⌘ P-Access-Network-Info changes		
<b>Source:</b>	⌘ Lucent Technologies		
<b>Work item code:</b>	⌘ IMS2	<b>Date:</b>	⌘ 21/10/2003
<b>Category:</b>	⌘ <b>D</b>	<b>Release:</b>	⌘ Rel-6
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		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)

<b>Reason for change:</b>	⌘ Examination of the contents of subclause 7.2A.4.3 leads to the conclusion that many of what are ostensibly called coding requirements are requirements on how the UE should code the header. This means that the contents are inappropriately placed in 24.229 and should be placed elsewhere, in addition to other changes that may be required by the IMSCOOP work item. The changes required for IMSCOOP mean that this text is also specific to the radio access technology, and therefore the text needs to be moved from the main body of the specification.
<b>Summary of change:</b>	⌘ A new subclause is created in Annex B relating to "application usage of SIP", which is intended to be subdivided as appropriate by functional entity. A single subclause is specified in this as "procedures for the UE". The existing text of subclause 7.2A.4. is substantially moved to the new subclause thus created, and modified to reflect a new introductory sentence "The UE shall populate...". The text in subclause 5.1 referring to the main text subclause 7.2A.4 is then modified to reference the new text, taking into account the fact that other access technologies may make use of this text.
<b>Consequences if not approved:</b>	⌘ Unclear specification, and text in the main body of the specification that is specific to GERAN and UTRAN.

<b>Clauses affected:</b>	⌘ 5.1.1.2, 5.1.1.3, 5.1.1.4, 5.1.1.6, 5.1.2A.1, 5.1.2A.2, 7.2A.4, B.3 (new)							
<b>Other specs</b>	⌘	<table border="1" style="display: inline-table; vertical-align: middle;"> <tr> <td style="text-align: center;">Y</td> <td style="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>	Y	N	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Other core specifications	⌘
Y	N							
<input type="checkbox"/>	<input checked="" type="checkbox"/>							

**affected:**

<input checked="" type="checkbox"/>	Test specifications
<input checked="" type="checkbox"/>	O&M Specifications

**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.

## PROPOSED CHANGE

### 5.1.1.2 Initial registration

The UE can register a public user identity at any time that a valid PDP context exists. 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.

A REGISTER request may be protected using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration.

The UE shall extract or derive from the UICC 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) the Authorization header, with the username field, set to the value of the private user identity;
- b) the From header set to the SIP URI that contains the public user identity to be registered;
- c) the To header set to the SIP URI that contains the public user identity to be registered;
- d) the Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;

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

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

- e) the 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.

- f) a Request-URI set to the SIP URI of the domain name of the home network;
- g) the Security-Client header field set to specify the security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];
- h) the Supported header containing the option tag "path"; and
- i) if a security association exists, a P-Access-Network-Info header [set as specified for the access network technology \(for GPRS see subclause B.3\)](#) ~~that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).~~

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

- a) store the expiration time of the registration for the public user identities found in the To header value;

- b) store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity;
- c) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header;
- d) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header;
- e) store the list of Service-Route headers contained in the Service-Route header, in order to build a proper preloaded Route header value for new dialogs; and
- f) 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.

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.

## PROPOSED CHANGE

### 5.1.1.3 Initial subscription to the registration-state event package

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the users registrar (S-CSCF) as described in draft-ietf-sipping-reg-event-00 [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; and
- f) a P-Access-Network-Info header set as specified for the access network technology (for GPRS see subclause B.3) that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

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.

## PROPOSED CHANGE

### 5.1.1.4 User-initiated re-registration

The UE can reregister a previously registered public user identity at any time.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less.

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

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

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

- a) an Authorization header, with the username field set to the value of the private user identity;
- b) a From header set to the SIP URI that contains the public user identity to be registered;
- c) a To header set to the SIP URI that contains the public user identity to be registered;
- d) a Contact header set to include SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected server port value bound to the security association;

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

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

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

NOTE 2: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

- f) a Request-URI set to the SIP URI of the domain name of the home network;
- g) a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];
- h) the Supported header containing the option tag "path"; and
- i) the P-Access-Network-Info header [set as specified for the access network technology \(for GPRS see subclause B.3\)](#) ~~that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).~~

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

- a) store the new expiration time of the registration for this public user identity found in the To header value;
- b) store the list of 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



- d) 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.

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.

## PROPOSED CHANGE

### 5.1.1.6 Mobile-initiated deregistration

The UE can deregister a previously registered public user identity at any time.

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

The UE shall extract or derive from the UICC 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) the Authorization header, with the username field, set to the value of the private user identity;
- b) the From header set to the SIP URI that contains the public user identity to be deregistered;
- c) the To header set to the SIP URI that contains the public user identity to be deregistered;
- d) the Contact header set to either the value of "\*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and the protected server port value bound to the security association;
- e) the Expires header, or the expires parameter of the Contact header, set to the value of zero, appropriate to the deregistration requirements of the user;
- f) a Request-URI set to the SIP URI of the domain name of the home network; and
- g) a P-Access-Network-Info header ~~that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4)~~ set as specified for the access network technology (for GPRS see subclause B.3).

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

If there are no more public user identities registered, the UE shall delete the security associations and related keys it may have towards the P-CSCF.

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

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

## PROPOSED CHANGE

### 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.

The UE shall discard any SIP message 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 of a NOTIFY request as a result of an implicit registration that was not subsequently deregistered or has expired; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

NOTE 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.

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

NOTE 3: The contents of the From header should not be relied upon to be modified by the network based on any privacy specified by the user either within the 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].

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 header as specified for the access network technology \(for GPRS see subclause B.3\)](#)~~This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).~~

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 port learnt during the registration procedure), and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

## 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.

The UE shall discard any SIP message 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.

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 header as specified for the access network technology \(for GPRS see subclause B.3\)](#) ~~This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).~~

# PROPOSED CHANGE

## 7.2A.4 ~~P-Access-Network-Info header~~ [Void](#)

### ~~7.2A.4.1 Introduction~~

~~The P-Access-Network-Info header is extended to include specific information relating to 3GPP access networks.~~

### ~~7.2A.4.2 Syntax~~

~~The syntax of the P-Access-Network-Info header is described in RFC 3455 [52].~~

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

~~In 3GPP systems, there are additional coding rules for the P-Access-Network-Info header:~~

~~If the *access type* field is equal to "3GPP-GERAN" the *access info* field shall contain a value for "egi-3gpp" parameter. This value shall be the Cell Global Identity obtained from lower layers of the UE.~~

~~The Cell Global Identity is a concatenation of MCC, MNC, LAC and CI (as described in 3GPP TS 23.003 [3]). The value of "egi-3gpp" parameter is therefore coded as a text string as follows:~~

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

~~If the *access type* field is equal to "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD" or "3GPP-CDMA2000" the *access info* field shall contain a value for "utran-cell-id-3gpp" parameter. This value shall be made up of a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003 [3]) and the UMTS Cell Identity (as described in 3GPP TS 25.331 [9A]), obtained from lower layers of the UE, and is coded as a text string as follows:~~

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

<b>PROPOSED CHANGE</b>
------------------------

---

## Annex B (normative): GPRS aspects when connected to the IM CN subsystem

### B.1 Scope

*Editor's note: To be drafted.*

---

### B.2 GPRS aspects when connected to the IM CN subsystem

#### B.2.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilise the services provided by GPRS to provide packet-mode communication between the UE and the IM CN subsystem.

Requirements for the UE on the use of these packet-mode services are specified in this clause. Requirements for the GGSN in support of this communication are specified in 3GPP TS 29.061 [11] and 3GPP TS 29.207 [12].

#### B.2.2 Procedures at the UE

##### B.2.2.1 PDP context activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

- a) perform a GPRS attach procedure;
- b) establish a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A]. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv6 address;

The UE shall choose one of the following options when performing establishment of this PDP context:

I. A dedicated PDP context for SIP signalling:

The UE shall indicate to the GGSN that this is a PDP context intended to carry IM CN subsystem-related signalling only by setting the IM CN Subsystem Signalling Flag. The UE may also use this PDP context for DNS and DHCP signalling according to the static packet filters as described in 3GPP TS 29.061 [11]. The UE can also set the Signalling Indication attribute within the QoS IE;

II. A general-purpose PDP context:

The UE may decide to use a general-purpose PDP Context to carry IM CN subsystem-related signaling. The UE shall indicate to the GGSN that this is a general-purpose PDP context by not setting the IM CN Subsystem Signalling Flag. The UE may carry both signalling and media on the general-purpose PDP context. The UE can also set the Signalling Indication attribute within the QoS IE.

The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message. Upon successful signalling PDP context establishment the UE receives an indication from

GGSN in the form of IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE. If the flag is not received, the UE shall consider the PDP context as a general-purpose PDP context.

The encoding of the IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE is described in 3GPP TS 24.008 [8].

The UE can indicate a request for prioritised handling over the radio interface by setting the Signalling Indication attribute (see 3GPP TS 23.107 [4A]). The general QoS negotiation mechanism and the encoding of the Signalling Indication attribute within the QoS IE are described in 3GPP TS 24.008 [8].

NOTE: A general-purpose PDP Context may carry both IM CN subsystem signaling and media, in case the media does not need to be authorized by Service Based Local Policy mechanisms defined in 3GPP TS 29.207 [12] and the media stream is not mandated by the P-CSCF to be carried in a separate PDP Context.

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] after PDP context activation.

The UE shall either:

- in the DHCP query, request a list of SIP server domain names of P-CSCF(s) and the list of Domain Name Servers (DNS); or
- request a list of SIP server IPv6 addresses of P-CSCF(s).

II. Transfer P-CSCF address(es) within the PDP context activation procedure.

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options IE of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

If the GGSN provides the UE with a list of P-CSCF IPv6 addresses in the ACTIVATE PDP CONTEXT ACCEPT message or ACTIVATE SECONDARY PDP CONTEXT ACCEPT message, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options IE as the P-CSCF address with the highest priority.

The UE can freely select method I or II for P-CSCF discovery. In case several P-CSCF addresses are provided to the UE, the selection of P-CSCF address shall be performed according to the resolution of host name as indicated in RFC 3261 [26]. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

The UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] or by the Protocol Configuration Options IE when activating a PDP context according to 3GPP TS 27.060 [10A].

The encoding of the request and response for IPv6 address(es) for DNS server(s) and list of P-CSCF address(es) within the Protocol Configuration Options IE is described in 3GPP TS 24.008 [8].

### B.2.2.1A Modification of a PDP context used for SIP signalling

The PDP context shall not be modified from a dedicated PDP context for SIP signalling to a general-purpose PDP context or vice versa. The IM CN Subsystem Signalling Flag shall not be set in the Protocol Configuration Options IE of the MODIFY PDP CONTEXT REQUEST message.

The UE shall not indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options IE of the MODIFY PDP CONTEXT REQUEST message. The UE shall ignore P-CSCF address(es) if received from the GGSN in the Protocol Configuration Options IE of the MODIFY PDP CONTEXT RESPONSE message.

## B.2.2.1B Re-establishment of the PDP context for signalling

If the dedicated PDP context for SIP signalling is lost due to e.g. a GPRS routing area update procedure, the UE shall attempt to re-establish the dedicated PDP context for SIP signalling. If this procedure does not succeed, the UE shall deactivate all PDP contexts established as a result of SIP signalling according to the 3GPP TS 24.008 [8].

## B.2.2.2 Session management procedures

The existing procedures for session management as described in 3GPP TS 24.008 [8] shall apply while the UE is connected to the IM CN subsystem.

## B.2.2.3 Mobility management procedures

The existing procedures for mobility management as described in 3GPP TS 24.008 [8] shall apply while the UE is connected to the IM CN subsystem.

## B.2.2.4 Cell selection and lack of coverage

The existing mechanisms and criteria for cell selection as described in 3GPP TS 25.304 [9] and 3GPP TS 44.018 [20] shall apply while the UE is connected to the IM CN subsystem.

## B.2.2.5 PDP contexts for media

### B.2.2.5.1 General requirements

The UE shall establish different PDP contexts for media streams that belong to different SIP sessions.

During establishment of a session, the UE establishes data stream(s) for media related to the session. Such data stream(s) may result in activation of additional PDP context(s). Such additional PDP context(s) shall be established as secondary PDP contexts associated to the PDP context used for signalling.

When the UE has to allocate bandwidth for RTP and RTCP in a PDP context, the UE shall use the rules outlined in 3GPP TS 29.208 [13].

#### B.2.2.5.1A Activation or modification of PDP contexts for media

If the UE receives indication within the SDP according to RFC 3524 [54] that media stream(s) belong to group(s), the media stream(s) shall be set up on separate PDP contexts according to the indication of grouping. The UE may freely group media streams to PDP context(s) in case no indication of grouping is received from the P-CSCF.

The UE can receive a media authorization token in the P-Media-Authorization header from the P-CSCF according to RFC 3313 [31]. The UE shall, if a media authorization token is received in the P-Media-Authorization header when a SIP session is initiated, establish separate PDP context(s) for the media. If a media authorization token is received in subsequent messages for the same SIP session, the UE shall:

- use the existing PDP context(s) for media;
- modify the existing PDP context(s) for media; or
- establish additional PDP context(s) for media.

The UE shall transparently pass the media authorization token received from the P-CSCF in the 183 (Session Progress) response to an INVITE request at originating setup or in the INVITE request at terminating setup to the GGSN. The UE shall signal it by inserting it within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message.

To identify to the GGSN which flow(s) (identified by m-lines within the SDP) that are transferred within a particular PDP context, the UE shall set the flow identifier(s) within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message. Detailed description of how the flow identifiers are constructed is provided in 3GPP TS 29.207 [12].

Detailed description of how the media authorization token and flow identifiers are carried in the Traffic Flow Template IE is provided in 3GPP TS 24.008 [8].

If the UE receives several media authorization tokens from the P-CSCF within the same SIP request or response, the first instance of the media authorization token shall be sent to the GGSN, and subsequent instances are discarded by the UE.

The UE shall not re-use a PDP context for other SIP sessions when the session has an associated media authorization token. The UE shall deactivate the PDP context when the SIP session that provided the media authorization token is terminated. When no media authorization token is used for a SIP session, the UE may reuse the PDP context between different SIP sessions.

The UE shall not include the IM CN Subsystem Signalling Flag when a PDP context for media is established or modified.

#### B.2.2.5.2 Special requirements applying to forked responses

Since the UE does not know that forking has occurred until a second, provisional response arrives, the UE sets up the PDP context(s) as required by the initial response received. If a subsequent provisional response is received, different alternative actions may be performed depending on the requirements in the SDP answer:

- 1) **the bearer requirements of the subsequent SDP can be accommodated by the existing PDP context(s).** The UE performs no activation or modification of PDP contexts.
- 2) **the subsequent SDP introduces different QoS requirements or additional IP flows.** The UE modifies the existing PDP context(s), if necessary, according to subclause B.2.2.5.1A.
- 3) **the subsequent SDP introduces one or more additional IP flows.** The UE establishes additional PDP context(s) according to subclause B.2.2.5.1A.

NOTE 1: When several forked responses are received, the resources requested by the UE are the “logical OR” of the resources indicated in the multiple responses to avoid allocation of unnecessary resources. The UE does not request more resources than proposed in the original INVITE request.

NOTE 2: When service-based local policy is applied, the UE receives the same authorization token for all forked requests/responses related to the same SIP session.

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall release all the unneeded radio/bearer resources. Therefore, upon the reception of a first final 200 (OK) response for the INVITE request (in addition to the procedures defined in RFC 3261 [26] subclause 13.2.2.4), the UE shall:

- 1) in case PDP context(s) were established or modified as a consequence of the INVITE request and forked provisional responses that are not related to the accepted 200 (OK) response, delete the PDP context(s) or modify the delete the PDP context(s) back to their original state.

#### B.2.2.5.3 Unsuccessful situations

One of the Go interface related error codes can be received by the UE in the ACTIVATE SECONDARY PDP CONTEXT REJECT message or the MODIFY PDP CONTEXT REJECT message. If the UE receives a Go interface related error code, the UE shall either terminate the session or retransmit the message up to three times. The Go interface related error codes are further specified in 3GPP TS 29.207 [12].

---

## B.3 Application usage of SIP

### B.3.1 Procedures at the UE

#### ~~7.2A.4.3~~ B.3.1.1 Additional coding rules for P-Access-Network-Info header

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

- 1) the access-type field set to one of "3GPP-GERAN", "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD" or "3GPP-CDMA2000" as appropriate to the radio access technology in use;
- 2) if the access type field is set to "3GPP-GERAN", a cgi-3gpp parameter set to the Cell Global Identity obtained from lower layers of the UE. The Cell Global Identity is a concatenation of MCC, MNC, LAC and CI (as described in 3GPP TS 23.003 [3]). The value of "cgi-3gpp" parameter is therefore coded as a text string as follows:

Starting with the most significant bit, MCC (3 digits), MNC (2 or 3 digits depending on MCC value), LAC (fixed length code of 16 bits using full hexadecimal representation) and CI (fixed length code of 16 bits using a full hexadecimal representation);
- 3) if the access type field is equal to "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD" or "3GPP-CDMA2000", a "utran-cell-id-3gpp" parameter set to a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003 [3]) and the UMTS Cell Identity (as described in 3GPP TS 25.331 [9A]), obtained from lower layers of the UE, and is coded as a text string as follows:

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