

**Source:** TSG CN WG 1  
**Title:** CRs to Rel-5 on Work Item IMS-CCR towards 24.229  
**Agenda item:** 8.1  
**Document for:** APPROVAL

---

**Introduction:**

This document contains 8 CRs on **Rel-5** on Work Item "IMS-CCR", that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #16 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Version Current	Version-New	Meeting-2nd-Level	Doc-2nd-Level
24.229	070	3	Rel-5	SDP procedures at UE	F	5.0.0	5.1.0	N1-24	N1-021453
24.229	073	2	Rel-5	Updates to the procedures involving the iFCs, following the Oulu iFC changes	F	5.0.0	5.1.0	N1-24	N1-021440
24.229	074	1	Rel-5	Addition of DHCPv6 references to 24.229	F	5.0.0	5.1.0	N1-SIP0204	N1-021086
24.229	075	1	Rel-5	Clarification to URL and address assignments	F	5.0.0	5.1.0	N1-SIP0204	N1-021083
24.229	079	3	Rel-5	Downloading the implicitly registered public user identities from the S-CSCF to P-CSCF	F	5.0.0	5.1.0	N1-24	N1-021510
24.229	080	3	Rel-5	Clarification of GPRS aspects	F	5.0.0	5.1.0	N1-24	N1-021486
24.229	081	2	Rel-5	Introduction of Subscription Locator Function Interrogation at I-CSCF in 24.229	F	5.0.0	5.1.0	N1-24	N1-021469
24.229	082	1	Rel-5	Introduction of Visited_Network_ID p-header	C	5.0.0	5.1.0	N1-24	N1-021433

CR-Form-v5

## CHANGE REQUEST

⌘ **24.229 CR 070** ⌘ rev **23** ⌘ Current version **5.0.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ SDP procedures at UE		
<b>Source:</b>	⌘ Nokia		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 07-05-2002
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ REL-5
	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)

<b>Reason for change:</b>	⌘ The changes resulted with the introduction of the UPDATE method and offer/answer SDP negotiation were not applied yet to this subclause.
<b>Summary of change:</b>	⌘ The CR deletes 3 statements not applicable any more and some editorial changes are done also.
<b>Consequences if not approved:</b>	⌘ The text in 6.1 will not be compliant with the offer/answer RFC and the new version of the Manyfolks and UPDATE draft.

<b>Clauses affected:</b>	⌘ 6.1
<b>Other specs affected:</b>	⌘ <input type="checkbox"/> Other core specifications ⌘ <input type="checkbox"/>
	<input type="checkbox"/> Test specifications ⌘ <input type="checkbox"/>
	<input type="checkbox"/> O&M Specifications ⌘ <input type="checkbox"/>
<b>Other comments:</b>	⌘ <input type="text"/>

### How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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 Application usage of SDP

### 6.1 Procedures at the UE

Usage of SDP by the UE:

1. An INVITE request generated by a UE ~~may shall~~ contain SDP payload. ~~In case preconditions will be used for session setup then SDP payload shall be present.~~ The SDP payload shall reflect the calling user UE#1's terminal capabilities and user preferences for the session. In addition, the calling user shall indicate the desired QoS for the session, using the segmented status type. ¶In an initial INVITE the UE shall indicate that it mandates local QoS, and that this precondition is not yet satisfied, i.e. the UE shall include the following preconditions:  
~~-----~~ a=des: qos mandatory local sendrecv  
~~-----~~ a=curr: qos local none

Editor's Note: The requirements for SDP payload in the case of Optimised Voice Mode are FFS.

2. The first 183 provisional response sent out shall contain the answer for the SDP received in the INVITE information. The SDP payload shall reflect the called user UE#2's terminal capabilities and user preferences.

Editor's Note: The case/action\_needed when a UE generates a 183 response without SDP payload is FFS.

3. When UE sends out an 183 with SDP payload, it shall ~~indicate the support for preconditions and in addition~~ request confirmation for the result of the resource reservation at the originating end point.

~~4. UE shall include SDP in the PRACK request for acknowledging the 183 Session Progress response if the codec negotiation during the INVITE request and 183 Session Progress response resulted in more than one codec per media line. It is recommended not to include any SDP payload if the SDP payload in the 183 Session Progress response contains only one codec information for each media line.~~

~~5. After the initial SDP has been sent the subsequent SDPs sent by the UE shall only contain a subset of the media descriptions of the initial SDP. In order to modify the media descriptors a reINVITE shall be used.~~

~~6. If Resource Reservation has been finished before sending the 200 OK for INVITE, then it shall contain the SDP payload that reflects the reserved resources on the radio interface.~~

7. During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description.

8. For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor in the SDP. For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208 [11].

9. The UE shall include the DTMF media format at the end of the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 2833 [17].

**3GPP TSG-CN1 Meeting #23**  
**Budapest, Hungary, 13. – 17. May 2002**

**Tdoc N1-021440**  
**Tdoc N1-021022**

CR-Form-v5

## CHANGE REQUEST

⌘ **TS 24.229 CR 073** ⌘ rev **2** ⌘ Current version: **5.0.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘	Updates to the procedures involving the iFCs, following the Oulu & Ft Lauderdale changes		
<b>Source:</b>	⌘	Ericsson		
<b>Work item code:</b>	⌘	IMS-CCR	<b>Date:</b>	⌘ 2002/05/14
<b>Category:</b>	⌘	<b>F</b>	<b>Release:</b>	⌘ REL-5
		Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
		<b>F</b> (correction)	<b>2</b>	(GSM Phase 2)
		<b>A</b> (corresponds to a correction in an earlier release)	<b>R96</b>	(Release 1996)
		<b>B</b> (addition of feature),	<b>R97</b>	(Release 1997)
		<b>C</b> (functional modification of feature)	<b>R98</b>	(Release 1998)
		<b>D</b> (editorial modification)	<b>R99</b>	(Release 1999)
		Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		<b>REL-4</b> (Release 4)
			<b>REL-5</b>	(Release 5)

<b>Reason for change:</b>	⌘	At the Oulu meeting, Siemens & al. clarified that the IFCs should be composed of triggers, to which there is a single AS assigned. That has been further clarified in Ft Lauderdale (N1-020953, CR 003R2). There is still in 24.229 procedures reminiscence of the days were the S-CSCF used to police contact messaging to the AS, ensuring that it would be contacted only once. As well, ServiceInformation is wrongly described as being unique, for one AS.		
<b>Summary of change:</b>	⌘	Clarify that: 1) the S-CSCF should not prevent a given AS to be contacted more than once, but according to the iFCs trigger. 2) There is one ServiceInformation per trigger.		
<b>Consequences if not approved:</b>	⌘	Internal specification inconsistencies leading to implementation divergence.		

<b>Clauses affected:</b>	⌘	5.4.3, 7.6.3		
<b>Other specs affected:</b>	⌘	<input type="checkbox"/> Other core specifications	⌘	
		<input type="checkbox"/> Test specifications		
		<input type="checkbox"/> O&M Specifications		
<b>Other comments:</b>	⌘	<a href="#">2002/05/14: update done to N1-021022 CR 73 Rev. -, at the editor's request. Identified with green marking.</a>		

**How to create CRs using this form:**

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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.

## 5.4.3 General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF

### 5.4.3.1 Requests initiated by the served user

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

- remove its own SIP URL from the topmost Route header;
- if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [16]) to a globally routable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [18]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or an appropriate SIP response shall be sent to the originator;
- check if <original-dialog-id> XML element is present in the payload of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;
- ~~check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous check, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:~~ check whether the initial request matches the initial filter criteria, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:
  - insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and
  - ~~initialise local data to track the status of contacting each application server specified in the service profile. Additionally, S-CSCF shall also~~ populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.
- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;
- determine the destination address (e.g. DNS access) using the URL placed in the topmost Route header if present, otherwise based on the Request-URI; and
- in case of an initial request for a dialog the S-CSCF shall create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed.

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and
- route the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and
- route the request based on the topmost Route header.

#### 5.4.3.2 Requests terminated at the served user

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

- remove its own URL from the topmost Route header;
- check if <original-dialog-id> XML element is present in the payload of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. ~~Local data shall be updated to indicate that this Application Server has been contacted for the initial request.~~ The S-CSCF shall determine the next hop using initial filter criteria ~~and local data on status of which Application Servers have been contacted.~~ If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;
- ~~check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous check the S-CSCF may contact one or more application server(s) before contacting an I-CSCF/P-CSCF respectively. In case of contacting one or more application server(s) the S-CSCF shall:~~ check whether the initial request matches the initial filter criteria, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:
  - insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and
  - ~~initialise local data to track the status of contacting each application server specified in the service profile.~~ **Additionally S-CSCF shall also** populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.
- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;
- in case there are no Route headers in the request, then determine, from the destination public user identity, the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2.1;
- determine, from the destination public user identity, the saved Contact URL where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2.1;
- build the Request-URI and Request header field values from the preloaded routes and saved Contact URL, as described in RFC 2543bis [20];
- insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;
- in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed;
- replace the Request-URI with the contents of the user Contact URL saved by the S-CSCF at registration time; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and
- forward the request based on the topmost Route header.



### 7.6.3 DTD description

This section describes the elements of the 3GPP IMS Document Type Definition.

- <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.
- <vnid>**: Visited network identifier. Optional element that describes the P-CSCF network name. The vnid value is a string of characters that identifies the P-CSCF network at the user's network home.
- <cell-id>**: This element describes the identity of the cell that is serving the user.
- The **<cell-id>** element contains the **<ran>** attribute that identifies the coding of the cell-id, according to whether the cell-id was received from the GERAN or UTRAN.
- The **<cell-id>** element comprises four children elements: **<mcc>**, **<mnc>**, **<lac>** and **<ci>**. They represent, respectively, the Mobile Country Code, Mobile Network Code, Location Area Code and Cell Identity, as described in [3].
- <original-dialog-id>**: The original dialog, as received by the S-CSCF. This element helps the S-CSCF to correlate dialogues when the Application Server is behaving as a B2BUA, and therefore, modifies then dialogue.
- The **<original-dialog-id>** element comprises three children elements: **<od-from>**, **<od-to>**, **<od-call-id>**. Their values contain, respectively, a copy of the From, To and Call-ID header values as received in the SIP message at the S-CSCF.
- <destination-public-user-id>**: The destination public-user-id URL of the current session.
- <access>**: The access element, if present, identifies the access that the UE is utilized to connect to the network. The element contains two children elements: **<ant>** and **<technology>**.
- The **<access-type>** child element describes the access type. The predefined values are:
- gprs: the user is accessing the network through a GRPS access;
  - wlan: the user is accessing the network through a wireless local area network;
  - fixed: the user is accessing the network through a fixed access.
- The **<technology>** child element, if present, describes the access technology. The pre-defined values are:
- utran: UTRAN, as defined in [3];
  - geran: GERAN, as defined in [3];
  - 802.11a: wireless local area network according to the 802.11a technology;
  - 802.11b: wireless local area network according to the 802.11b technology;
  - sat: satellite access;
  - adsl: asymmetric digital subscriber line.
- <charging-vector>**: the charging-vector element, if present, identifies charging correlation information. The element contains two children elements: **<icid>** and **<gprs-charging-id>**.
- The **<icid>** child element contains an IMS charging identifier that is globally unique and is associated with the end-to-end session.
- The **<gprs-charging-id>** child element, if present, contains GPRS charging identifiers comprised of the following: **<ggsn>** and **<pdp-info>**:
- **<ggsn>**: identifier of the GGSN;

- <pdp-info>: one or more instances of information for a PDP context, which is comprised of two children elements: <pdp-index> and <pdp-id>:
  - <pdp-index>: relative index of PDP context as it correlates to a media stream in the SDP;
  - <pdp-id>: unique identifier of the PDP context from the GGSN.

<service-info>: the transparent element received from the HSS for a particular ~~Application Server~~[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.

## CHANGE REQUEST

⌘ **24.229 CR 074** ⌘ rev **1** ⌘ Current version: **5.0.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Addition of the DHCPv6 related IETF documents		
<b>Source:</b>	⌘ Ericsson		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 24-Apr-02
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ REL-5
	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 TR 21.900.		Use <u>one</u> of the following releases: 2 (GSM Phase 2) R96 (Release 1996) R97 (Release 1997) R98 (Release 1998) R99 (Release 1999) REL-4 (Release 4) REL-5 (Release 5)

<b>Reason for change:</b>	⌘ There are no references to the DHCPv6 procedures in 24.229		
<b>Summary of change:</b>	⌘ Addition of the references to DHCPv6 and DHCPv6 options for SIP servers		
<b>Consequences if not approved:</b>	⌘ Missunderstanding about the standard to implement		

<b>Clauses affected:</b>	⌘ 2, 9.2.1		
<b>Other specs affected:</b>	<input checked="" type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘ 24.228	
<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/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.htm). Below is a brief summary:

- 1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

\*\*\*\*\* **First proposed 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".
  - [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".
  - [10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".
  - [11] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".
  - [12] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx Interface; Signalling flows and message contents".
  - [13] 3GPP TS 33.102: "3G Security; Security architecture".
  - [14] 3GPP TS 33.203: "Access security for IP based services".
  - [15] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".
  - [16] RFC 2806: "URLs for Telephone Calls".
  - [17] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".
  - [18] RFC 2916: "E.164 number and DNS".
  - [19] RFC 2976 (October 2000): "The SIP INFO method".
  - [20] draft-ietf-sip-rfc2543bis-07 (January 2002): "SIP: Session Initiation Protocol".
- Editor's note: The above document cannot be formally referenced until it is published as an RFC.
- [21] draft-ietf-sip-100rel-05 (February 2002): "Reliability of provisional responses in SIP".

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

[22] draft-sip-manyfolks- resource-03 (November 2001): "Integration of resource management and SIP".

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

[23] draft-ietf-sip-events-02.txt (February 2002): "SIP-Specific Event Notification".

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

[24] draft-ietf-sip-callerprefs-05 (November 2001): "SIP caller preferences and callee capabilities".

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

[25] draft-ietf-sip-refer-02 (October 2001): "The REFER method".

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

[26] draft-ietf-sip-session-timer-08 (October 2001): "The SIP session timer".

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

[27] draft- sip-privacy-03 (November 2001): "SIP extensions for caller identity and privacy".

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

[28] draft- sip-state-02 (August 2001): "SIP extensions for supporting distributed call state".

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

[29] draft- sip-call-auth-03 (November 2001): "SIP extensions for media authorization".

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

[30] draft-ietf-mmusic-sdp-new-04 (November 2001): "SDP: Session Description Protocol".

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

[30A] draft-ietf-dhc-dhcpv6-23 (February 2002): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)"

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

[30B] draft-ietf-sip-dhcpv6-00 (April 2002): "DHCPv6 options for SIP servers"

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

---

### 3 Definitions and abbreviations

**\*\*\*\*\* Next proposed change \*\*\*\*\***

## 9.2 Procedures at the UE

### 9.2.1 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]. 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 an IPv6 address. This PDP context can be either a primary or a secondary PDP context;

Editor's note: Actual APN values for IMS are yet not determined.

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

The methods for P-CSCF discovery are:

- I. Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) ~~DHCP~~ [30A], the DHCPv6 options for SIP servers [30B] and if needed DNS 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 when activating the PDP context.

If the GGSN provides the UE with a list of P-CSCF IPv6 addresses, 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 coding of the Protocol Configuration Options IE is described in 3GPP TS 24.008 [8].

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 2543bis [20]. 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 in the PDP context activation 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.

CR-Form-v5

## CHANGE REQUEST

⌘ **24.229 CR 075** ⌘ rev **1-** ⌘ Current version: **5.0.0** ⌘

For [HELP](#) on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Clarification to URL and address assignments		
<b>Source:</b>	⌘ Nokia		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 2418-04-2002
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ REL-5
	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>Reason for change:</b>	⌘ Clarification of address allocation of IM CN subsystem entities		
<b>Summary of change:</b>	⌘ IM CN subsystem entities may be allocated SIP URLs instead of FQDNs		
<b>Consequences if not approved:</b>	⌘ Inconsistent implementations		

<b>Clauses affected:</b>	⌘ <a href="#">3.2</a> , <a href="#">4.2</a> , <a href="#">5.2.3</a> , <a href="#">5.4.1.2.1</a> , <a href="#">5.4.1.4</a> , <a href="#">5.4.1.7</a>		
<b>Other specs affected:</b>	<input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> 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/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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.

## 3.2 Abbreviations

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

1xx	A status-code in the range 101 through 199, and excluding 100
2xx	A status-code in the range 200 through 299
AS	Application Server
AUTN	Authentication TokeN
BGCF	Breakout Gateway Control Function
c	conditional
CK	Ciphering Key
CN	Core Network
CSCF	Call Session Control Function
DNS	Domain Name System
<del>FQDN</del>	<del>Fully Qualified Domain Name</del>
i	irrelevant
I-CSCF	Interrogating CSCF
IK	Integrity Key
IM	IP Multimedia
IP	Internet Protocol
ISC	IP multimedia Subsystem Service Control
m	mandatory
MAC	Message Authentication Code
MGCF	Media Gateway Control Function
MRFC	Media Resource Function Controller
n/a	not applicable
o	optional
P-CSCF	Proxy CSCF
PDU	Protocol Data Unit
RAND	RANDom challenge
RES	RESponse
RTP	Real-time Transport Protocol
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SQN	SeQuence Number
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UE	User Equipment
URI	Universal Resource Identifier
URL	Universal Resource Locator
x	prohibited

-----Next modification-----

## 4.2 URL and address assignments

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

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

**Editor's note: The requirements for DNS-SRV entries or alternatives require further discussion.**



- 2) All IM CN subsystem entities are allocated IP addresses. Allocation of IPv6 and IPv4 addresses fulfils the requirements of of 3GPP TS 23.221 [6] subclause 5.1.
- 3) The subscriber is allocated a private user identity by the home network operator, and this is contained within the USIM. This private user identity is available to the SIP application within the UE.

NOTE: The ~~FQDNs-SIP URLs~~ may be resolved by using any of public DNSs, private DNSs, or peer-to-peer agreements.

- 4) The subscriber is allocated one or more public user identities by the home network operator. At least one of these is contained within the USIM. All public user identities are available to the SIP application within the UE.
- 5) The UE is dynamically assigned an IP version 6 address.

-----Next modification-----

### 5.2.3 Subscription to the users registration-state event package

Upon receipt of a 2xx response to the initial REGISTER request of an user, the P-CSCF shall subscribe to the users registration-state event package at the users registrar (S-CSCF). Therefore the P-CSCF shall generate a SUBSCRIBE request with the following elements:

- a Request-URI set to the topmost entry of the path information that was obtained during the users registration;
- a From header set to ~~a~~ the P-CSCF's SIP URL; ~~that contains the P-CSCF's FQDN;~~
- a To header, set to a SIP URL that contains the public user identity that was previously registered;
- an Event header set to the "registration-state" event package;
- an Expires header set to a value higher then the Expires header of the before sent REGISTER request from the user; and
- a Route header according to the path information that was obtained during the users registration. Th S-CSCF shall set the last Route header entry to the resource to which it wants to subscribe to, i.e. to a SIP URL the public user identity that was previously registered.

Afterwards the P-CSCF shall send out the so generated SUBSCRIBE request.

Upon receipt of a 2xx response to the SUBSCRIBE message, the P-CSCF shall store the information for the so established dialog and the expiration time as indicated in the Expires header of the received response.

-----Next modification-----

#### 5.4.1.2.1 Normal procedures

When the S-CSCF receives a REGISTER request, the S-CSCF shall verify that the "path" option-tag is contained in the Proxy-Require header. If the "path" option-tag is present, the S-CSCF shall store the information contained in the Path header so that it can be used for mobile terminated requests.

**Editor's Note: If the S-CSCF receives a Path header without the "path" option tag in the Proxy-Require header, we have an error condition in the I-CSCF. The I-CSCF behavior for this scenario is FFS.**

The S-CSCF shall:

- check the existence of a Path header in the request;

**Editor's note: The action S-CSCF has to take when a Path header is not present in the request is FFS.**

- when a Path header exists in the request, insert its own FQDNSIP URL, ~~or IP address, in the form of SIP URL~~ at the top of the list found in the Path header saved from the REGISTER request;
- save the Contact header value for the entire duration of the registration;

- construct a list of preloaded Route headers from the list of entries in the Path header. The order in the lists is preserved;
- include an expiration time in the 200 OK response, using one value provided within the S-CSCF, according to the local policy of the network, if this expiration time is shorter than the requested expiry time received from the UE;
- save the list of preloaded Route headers for the entire duration of the registration;

NOTE 1: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

- bind to each individual public user identity all contact information under which the public user identity has been registered (either manually by means of a REGISTER message or automatically upon the registration of another public user identity);

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

- bind to each contact information the respective Path header entries, that were received in the same REGISTER message as that contact information;
- add its Path header on the top of the received list of Path headers, and returns this list in the 200 OK response;
- check whether the message contains information indicating that it was received with a valid integrity check by the P-CSCF; and

**Editor's Note: The method by which the P-CSCF indicates this is FFS.**

- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

On receiving a failure response to one of the third-party REGISTER requests, the S-CSCF may initiate network-initiated deregistration procedure based on the information in the Filter Criteria. If the Filter Criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the Application Server, the S-CSCF shall not initiate network-initiated deregistration procedure.

The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for initial registration. The information that a REGISTER has a valid integrity check may be used as part of the decision to authenticate the registration. The S-CSCF shall request authentication by responding to the REGISTER request with a 401 Unauthorized with:

- the Authorization header containing the authentication parameters (RAND, AUTN, CK and IK).

-----Next modification-----

#### 5.4.1.4 User-initiated deregistration

When the S-CSCF receives a REGISTER request, it shall verify that the "path" option-tag is contained in the Proxy-Require header. If the "path" option-tag is present, the S-CSCF shall store the information contained in the Path header so that it can be used for mobile terminated requests.

**Editor's Note: If the S-CSCF receives a Path header without the "path" option tag in the Proxy-Require header, we have an error condition in the I-CSCF. The I-CSCF behavior for this scenario is FFS.**

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

- deregister the subscriber and remove all related stored information;
- insert its own ~~FQDN SIP URL~~ or IP address in the form of SIP URL at the top of the list found in the Path header saved from the REGISTER request;
- add its Path header on the top of the received list of Path headers, and returns this list in the 200 OK response; and

- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

-----Next modification-----

#### 5.4.1.7 Notification of Application Servers about registration status

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 Application Server with the following information:

- a) the Request-URI shall contain the ~~AS's FQDN SIP URL~~ or IP address of the AS in the form of a SIP URL;
- b) the From header shall contain the ~~S-CSCF's FQDN SIP URL~~ or IP address of the S-CSCF in the form of a SIP URL;
- c) the To header shall contain the public user identity as contained in the REGISTER request received from the UE;
- d) the Contact header shall contain the ~~S-CSCF's FQDN SIP URL~~ or IP address of the S-CSCF in the form of a SIP URL;
- e) for initial registration and user-initiated reregistration (subclause 5.4.1.2), the Expires header 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 shall contain the value zero;
- g) for initial registration and user-initiated reregistration (subclause 5.4.1.2), a message body shall be included in the REGISTER request 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 IM SSF). If there is a service information XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [12]), then it shall be included in the REGISTER message body within the <service-info> XML element as described in subclause 7.6. For the messages including the 3GPP IMS XML body, set the value of the Content-Type header to include the MIME type specified in subclause 7.6.

CR-Form-v5

## CHANGE REQUEST

⌘ **24.229 CR 079** ⌘ rev **3** ⌘ Current version: **5.0.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Downloading the list of public user identities with P-Associated-URI		
<b>Source:</b>	⌘ Nokia, Siemens, Ericsson, Nortel, Dynamicsoft		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 17-May-2002
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ REL-5
	<i>Use one of the following categories:</i> <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> .		<i>Use one of the following releases:</i> <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>Reason for change:</b>	⌘ With the current solution the UE will get the implicitly registered public IDs once it has subscribed to its own registration information.
<b>Summary of change:</b>	⌘ A new P-Associated-URI header has been added to the 200 OK response to REGISTER requests. The S-CSCF will insert the list of associated public user identities into this header. The P-CSCF and the UE will store the content of it.
<b>Consequences if not approved:</b>	⌘ The UE will get the list of implicitly public user identities in a NOTIFY, but it will not get the non registered IDs. If the ISIM application is not present, the UE will not have a valid public user identity to subscribe to its own registration-state.

<b>Clauses affected:</b>	⌘ 5.1.1.2, 5.1.1.4, 5.2.2, 5.4.1.2.1, 5.4.1.5		
<b>Other specs affected:</b>	⌘ <input checked="" type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘ 24.228 (CR 028)	
<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/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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 Procedures at the UE

### 5.1.1 Registration and authentication

#### 5.1.1.1 General

The UE shall register public user identities (see table A.3/1 and dependencies on that major capability).

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

#### 5.1.1.2 Initial registration

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

A REGISTER request may be integrity protected using IK, see 3GPP TS 33.203 [14], received in an earlier registration.

The public user identity to be registered can be extracted either from the USIM or may be input from the end user. On sending a REGISTER request, the UE shall populate the header fields as follows:

- a) the user ID field of the authentication protocol, carried in the Authorization header, shall contain the private user identity. This shall be extracted from the USIM;
- b) the From header shall contain the public user identity to be registered;
- c) the To header shall contain the public user identity to be registered;
- d) the Expires header, or the expires parameter within the Contact header, shall contain 600 000 seconds as the value desired for the duration of the registration.

NOTE: 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 response.

The use of the Path header shall not be supported by the UE.

On receiving the 200 OK response to the REGISTER request, the UE shall store the expiration time of the registration for the public user identities found in the To: header value. The UE shall also 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.

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 Registration 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 response.

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

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the users registration-state event package for the public user identity registered as described in subclause 5.1.1.2 at the users registrar (S-CSCF). Therefore the UE shall generate a SUBSCRIBE request with the following elements:

- a Request URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URL that contains the public user identity that was previously registered;
- a From header set to a SIP URL that contains the public user identity that was previously registered;
- a To header, set to a SIP URL that contains the public user identity that was previously registered;

- an Event header set to the "registration-state" event package;
- an Expires header set to a value higher than the Expires header of the before sent REGISTER request.

Afterwards it shall send out the so generated SUBSCRIBE request.

Upon receipt of a 2xx response to the SUBSCRIBE message, the UE shall store the information for the established dialog and the expiration time as indicated in the Expires header of the received response.

The UE shall automatically resubscribe to the registration-state event package for a previously registered public user identity if the expiration time, as indicated in the Expires header of the 2xx response to the SUBSCRIBE message, has run out and the public user identity is still registered.

#### 5.1.1.4 User-initiated re-registration

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

The UE shall reregister the public user identity 600 seconds before the expiration time of a previous registration, unless either the user or the application within the UE has determined that a continued registration is not required. If the registration period indicated from the S-CSCF is less than 600 seconds, the UE shall reregister when half of the registration period has expired.

The REGISTER request may be integrity protected using IK, see 3GPP TS 33.203 [14], received in an earlier registration.

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

- a) the user ID field of the authentication protocol, carried in the Authorization header, shall contain the private user identity. This shall be extracted from the USIM;
- b) the From header shall contain the public user identity to be registered;
- c) the To header shall contain the public user identity to be registered;
- d) the Expires header, or the expires parameter within the Contact header, should contain the same expiration timer as the expiration timer returned in the 200 OK response to the initial.

NOTE: 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 response.

On receiving the 200 OK response to the REGISTER request, the UE shall store the new expiration time of the registration for this public user identity found in the To: header value. The UE shall also 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.

The use of the Path header shall not be supported by the UE.

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 Registration 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 response.

#### 5.1.1.5 Authentication

##### 5.1.1.5.1 General

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

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

- check the validity of a received authentication challenge, as described in 3GPP TS 33.102 [13] i.e. the locally calculated MAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range.

In the case that the 401 Unauthorized response is deemed to be valid the UE shall:

- extract the RAND and AUTN parameters, and use the derived keys (CK and IK) to protect future messages, see 3GPP TS 33.203 [14]; and
- send another REGISTER request using the derived IK to integrity protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the private user identity and the authentication challenge response (RES parameter).

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

#### **5.1.1.5.2 Network-initiated re-authentication**

Upon receipt of a NOTIFY message on the dialog which was generated during subscription to the registration-state event package, which contains the registration state value "re-authenticate" for a public user identity, the UE shall start the re-authentication procedures by initiating a reregistration as described in subclause 5.1.1.4.

#### **5.1.1.5.3 Abnormal cases**

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

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER shall contain no response parameter (e.g. no RES or AUTS);
- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER shall contain the AUTS parameter (see 3GPP TS 33.102 [13]).

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

#### **5.1.1.6 Mobile-initiated deregistration**

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

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

- a) the user ID field of the authentication protocol, carried in the Authorization header, shall contain the private user identity. This shall be extracted from the USIM;
- b) the From header shall contain the public user identity to be deregistered;
- c) the To header shall contain the public user identity to be deregistered;
- d) the Expires header, or the expires parameter of the Contact header, shall contain a value of zero, appropriate to the deregistration requirements of the user.

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

#### **5.1.1.7 Network-initiated deregistration**

Upon receipt of a NOTIFY message on the dialog which was generated during subscription to the registration-state event package as described in subclause 5.1.2.1, which contains the registration state value "closed", i.e. deregistered,



for one or more public user identities that were previously stored as registered, the UE shall remove all registration details relating to these public user identities.

**Editor's Note: The actions to be taken by the UE if all public user identities of one user have been deregistered are for further study, e.g. releasing signalling PDP context, information to the user, etc.**

**\*\*\*\*\* Next proposed change \*\*\*\*\***

## 5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE that pertains to a given public user identity, the P-CSCF shall:

- insert a Path header in the request. The P-CSCF shall include in the Path header an entry containing the SIP URL identifying the P-CSCF;
- insert a Require header and a Proxy-Require header both containing the option tag "path";
- if the REGISTER request was received with a valid integrity check, add information to the REGISTER request to indicate that the REGISTER request was received with a valid integrity check; and

**Editor's Note : The exact mechanism for this is FFS.**

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

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

- 1) remove its SIP URL from the list of Path headers, reverses the order of the list and save the resulting list of Path headers. This list shall be stored during the entire registration period of the respective public user identity. This list shall be used to preload the routing information into the initial requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing Path headers with the new list;
- 2) associate the Path header information with the registered public user identity;
- 3) remove the list of Path headers and "path" option-tags from the 200 OK response before forwarding the response to the UE;
- 4) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE.

When the P-CSCF receives a 401 Unauthorized response to a REGISTER request, the P-CSCF shall remove and store the CK and IK values contained in the 401 Unauthorized response. The 401 Unauthorized response shall be forwarded to the UE if and only if the CK and IK have been removed.

**Editor's Note: The P-CSCF behaviour when 3xx or 4xx responses other than 401 Unauthorized are received is FFS.**

**Editor's Note: The text above assumes that public user identities are registered one by one. Public user identity might need to be changed to Service Profile in the case when public user identities can be implicitly registered.**

**NOTE:** The P-CSCF will maintain two Route lists. The first Route list - created during the registration procedure - is used only to pre-load the routing information into the initial INVITE request that originated at the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

When the P-CSCF receives a 420 Bad Extension response to the above REGISTER request, the P-CSCF shall check the value of the Unsupported header field. When the value of the Unsupported header field is path, the P-CSCF shall take OA&M actions to indicate an error, in addition to passing on the 420 response to the UE. In all other cases, the P-CSCF shall proxy the 420 Bad Extension response.

### 5.2.3 Subscription to the users registration-state event package

Upon receipt of a 2xx response to the initial REGISTER request of an user, the P-CSCF shall subscribe to the users registration-state event package at the users registrar (S-CSCF). Therefore the P-CSCF shall generate a SUBSCRIBE request with the following elements:

- a Request-URI set to the topmost entry of the path information that was obtained during the users registration;
- a From header set to a SIP URL that contains the P-CSCF's FQDN;
- a To header, set to a SIP URL that contains the public user identity that was previously registered;
- an Event header set to the "registration-state" event package;
- an Expires header set to a value higher then the Expires header of the before sent REGISTER request from the user; and
- a Route header according to the path information that was obtained during the users registration. Th S-CSCF shall set the last Route header entry to the resource to which it wants to subscribe to, i.e. to a SIP URL the public user identity that was previously registered.

Afterwards the P-CSCF shall send out the so generated SUBSCRIBE request.

Upon receipt of a 2xx response to the SUBSCRIBE message, the P-CSCF shall store the information for the so established dialog and the expiration time as indicated in the Expires header of the received response.

### 5.2.4 Registration of multiple public user identites

Upon receipt of a NOTIFY message on the dialog which was generated during subscription to the registration-state event package, the P-CSCF shall perform the following actions:

- if a registration state value "open", i.e. registered is received for one or more public user identities, the P-CSCF shall bind the indicated public user identities as registered to the contact information of the user;
- if a registration state value "closed", i.e. deregistered is received for one or more public user identities, the P-CSCF shall release all stored information for these public user identities.

NOTE: There may be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity. These automatically registered public user identities belong to the same service profile of the user and they are not available at the P-CSCF, i.e. P-CSCF does not know that they have been registered. The here-described procedures provide a mechanism to inform the UE about these automatically registered public user identities.

### 5.2.5 Deregistration

#### 5.2.5.1 User-initiated deregistration

When the P-CSCF receives a 200 OK response to a REGISTER request (sent according to subclause 5.2.2), it shall check the value of the Expires header field and/or expires parameter in the Contact header field. When the value of the Expires header field or expires parameter equals zero, then the P-CSCF shall remove the public user identity found in the To header field, and all the associated public user identities, from the registered public user identities list and all related stored information.

NOTE: There is no requirement to distinguish a REGISTER request relating to a registration from that relation to a deregistration. For administration reasons the P-CSCF may distinguish such requests, however this has no impact on the SIP procedures.

\*\*\*\*\* Next proposed change \*\*\*\*\*

## 5.4.1 Registration and authentication

### 5.4.1.1 Introduction

The S-CSCF shall act as the SIP registrar for all UAs of the IM CN subsystem with public user identities, (see table A.150/2 and other capabilities in annex A dependent on that major capability).

The S-CSCF shall support the use of the Path header. The S-CSCF must also support the Require and Proxy-Require headers. The Path header is only applicable to the REGISTER request and its 200-OK response.

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

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

### 5.4.1.2 Initial registration and user-initiated reregistration

#### 5.4.1.2.1 Normal procedures

When the S-CSCF receives a REGISTER request, the S-CSCF shall verify that the "path" option-tag is contained in the Proxy-Require header. If the "path" option-tag is present, the S-CSCF shall store the information contained in the Path header so that it can be used for mobile terminated requests.

**Editor's Note: If the S-CSCF receives a Path header without the "path" option tag in the Proxy-Require header, we have an error condition in the I-CSCF. The I-CSCF behavior for this scenario is FFS.**

The S-CSCF shall:

- check the existence of a Path header in the request;

**Editor's note: The action S-CSCF has to take when a Path header is not present in the request is FFS.**

- when a Path header exists in the request, insert its own FQDN, or IP address, in the form of SIP URL at the top of the list found in the Path header saved from the REGISTER request;
- save the Contact header value for the entire duration of the registration;
- construct a list of preloaded Route headers from the list of entries in the Path header. The order in the lists is preserved;
- include an expiration time in the 200 OK response, using one value provided within the S-CSCF, according to the local policy of the network, if this expiration time is shorter than the requested expiry time received from the UE;
- save the list of preloaded Route headers for the entire duration of the registration;

NOTE 1: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

- bind to each individual public user identity all contact information under which the public user identity has been registered (either manually by means of a REGISTER message or automatically upon the registration of another public user identity);

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

- bind to each contact information the respective Path header entries, that were received in the same REGISTER message as that contact information;
- add its Path header on the top of the received list of Path headers, and returns this list in the 200 OK response;

- [include a P-Associated-URI header containing the list of public user identities that the user is authorized to use. Such a collection of public user identities may or may not be implicitly registered by the network;](#)

- check whether the message contains information indicating that it was received with a valid integrity check by the P-CSCF; and

**Editor's Note: The method by which the P-CSCF indicates this is FFS.**

- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

On receiving a failure response to one of the third-party REGISTER requests, the S-CSCF may initiate network-initiated deregistration procedure based on the information in the Filter Criteria. If the Filter Criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the Application Server, the S-CSCF shall not initiate network-initiated deregistration procedure.

The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for initial registration. The information that a REGISTER has a valid integrity check may be used as part of the decision to authenticate the registration. The S-CSCF shall request authentication by responding to the REGISTER request with a 401 Unauthorized with:

- the Authorization header containing the authentication parameters (RAND, AUTN, CK and IK).

#### 5.4.1.2.2 Abnormal cases

In the case that the authentication response from the UE is incorrect the S-CSCF shall either:

- attempt a further authentication challenge; or
- deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the response from the UE is incorrect for three consecutive attempts then the S-CSCF shall deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), the S-CSCF shall either:

- attempt a further authentication challenge; or
- deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the response from the UE indicates that the authentication challenge was invalid with no RES or AUTS parameter in the subsequent REGISTER message, the S-CSCF shall:

- respond with the relevant 4xx response (e.g. 401 Unauthorized to initiate a further authentication attempt, or 403 Forbidden if the authentication attempt is to be abandoned).

In the case that the response from the UE indicates that the authentication challenge was invalid with the AUTS parameter in the subsequent REGISTER message, the S-CSCF shall:

- fetch new authentication vectors from the HSS, including AUTS and RAND in the request to indicate a resynchronisation; and
- on receipt of the new vectors send a 401 Unauthorized to initiate a further authentication attempt, using these new vectors.

In the case that the expiration timer from the UE is too short to be accepted by the S-CSCF, the S-CSCF shall:

- reject the REGISTER with a 423 Registration Too Brief, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

#### 5.4.1.3 Authentication and reauthentication

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

#### 5.4.1.4 User-initiated deregistration

When the S-CSCF receives a REGISTER request, it shall verify that the "path" option-tag is contained in the Proxy-Require header. If the "path" option-tag is present, the S-CSCF shall store the information contained in the Path header so that it can be used for mobile terminated requests.

**Editor's Note: If the S-CSCF receives a Path header without the "path" option tag in the Proxy-Require header, we have an error condition in the I-CSCF. The I-CSCF behavior for this scenario is FFS.**

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

- deregister the ~~subscriber~~ [public user identity found in the To: header field together with the implicitly registered public user identities](#), and remove all related stored information;
- insert its own FQDN or IP address in the form of SIP URL at the top of the list found in the Path header saved from the REGISTER request;
- add its Path header on the top of the received list of Path headers, and returns this list in the 200 OK response; and
- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

#### 5.4.1.5 Network-initiated deregistration

When a network-initiated deregistration event occurs for a public user identity, and the UE has subscribed for that event, the S-CSCF shall generate a NOTIFY request in order to inform the UE of the network-initiated deregistration event for that public user identity. The S-CSCF shall set the event header to the name of the event package, which provides information about the registration state of the UE.

When a network-initiated deregistration event occurs for a public user identity, and the P-CSCF has subscribed for registration events for that public user identity, the S-CSCF shall generate a NOTIFY request in order to inform the P-CSCF of the network initiated deregistration event for that public user identity. The S-CSCF shall set the event header to the name of the event package, which provides information about the registration state of the UE.

If the network-initiated deregistration is for a set of public user identities associated with the subscriber, the NOTIFY shall send the registration state of all public user identities of the subscriber.

**Editor's note: The possible values of the event header are: presence, registration-state, a new subpackage of presence.**

Also, the S-CSCF shall send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event.

[The S-CSCF shall then de-register the public user identity together with the implicitly registered public user identities.](#)

#### 5.4.1.6 Network-initiated reauthentication

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

If the S-CSCF is informed that a private user identity needs to be re-authenticated, the S-CSCF shall generate a NOTIFY request on all dialogs (i.e. the dialog between S-CSCF and the UE and additionally between S-CSCF and P-CSCF) which have been established due to subscription to the registration-state event package of that user. The S-CSCF shall populate the content of the NOTIFY request and additionally shall:

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

- set the Event header to the "registration-state" value; and
- indicate a public user identity of the user for which the private user identity needs to be re-authenticated in the body of the NOTIFY request with registration state "re-authenticate".

Afterwards the S-CSCF shall:

- wait for the user to reauthenticate (see subclause 5.4.1.2).

NOTE: Network initiated re-authentication might be requested from the HSS or may occur due to internal processing within the S-CSCF.

In case S-CSCF receives no data it can authenticate the subscriber from, the S-CSCF may as an implementation option try to request the UE by other means to re-authenticate, e.g. by sending a REFER method in order to request a REGISTER message.

If UE does not re-authenticate within a certain period of time, the S-CSCF shall deregister the private user identity as described in subclause 5.4.1.5 and terminate the ongoing sessions of that user.

#### 5.4.1.7 Notification of Application Servers about registration status

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 Application Server with the following information:

- a) the Request-URI shall contain the FQDN or IP address of the AS in the form of a SIP URL;
- b) the From header shall contain the FQDN or IP address of the S-CSCF in the form of a SIP URL;
- c) the To header shall contain the public user identity as contained in the REGISTER request received from the UE;
- d) the Contact header shall contain the FQDN or IP address of the S-CSCF in the form of a SIP URL;
- e) for initial registration and user-initiated reregistration (subclause 5.4.1.2), the Expires header 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 shall contain the value zero;
- g) for initial registration and user-initiated reregistration (subclause 5.4.1.2), a message body shall be included in the REGISTER request 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 IM SSF). If there is a service information XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [12]), then it shall be included in the REGISTER message body within the <service-info> XML element as described in subclause 7.6. For the messages including the 3GPP IMS XML body, set the value of the Content-Type header to include the MIME type specified in subclause 7.6.

### 5.4.2 Subscription and notification

*Editors Note: This should be handled in a generic way*

#### 5.4.2.1 Subscriptions to S-CSCF events

##### 5.4.2.1.1 Subscription to the event providing registration state

When an incoming SUBSCRIBE request addressed to S-CSCF arrives containing the Event header with the registration-state event package, the S-CSCF shall generate a 2xx response acknowledging the SUBSCRIBE request and indicating that the subscription was successful. Furthermore, the response shall include:

- an Expires header which either contains the same or a decreased value as the Expires in SUBSCRIBE request; and

- a Contact header which is an identifier generated within the S-CSCF that will help to correlate refreshes for the SUBSCRIBE.

**Editor's note: Authorization needs to be applied before subscribing for the event providing information about the registration state. This is FFS.**

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

#### 5.4.2.1.2 Notification about registration state

If the registration state of one or more public user identities changes, the S-CSCF shall generate a NOTIFY request on all dialogs which have been established due to subscription to the registration-state event package of that user. For each NOTIFY request, the S-CSCF shall:

- set the Request-URI and Route header to the saved route information during subscription;
- set the Event header to the "registration-state" value;
- indicate registration state "open" for all public user identities which are currently registered;
- indicate registration state "closed" for all public user identities which are currently deregistered; and
- indicate within the "<detail>" information of those public user identities which will be automatically reregistered the "automatically by" information, followed by the specific public user identity which will cover the reregistration.

**EXAMPLE:** If sip:user1\_public1@home1.net is reregistered, the public user identity sip:user1\_public2@home1.net **can** be registered. Therefore the entries in the body of the NOTIFY message look like:

```
<tuple name="sip:user1_public1@home1.net">
  <status><value>open</value></status>
</tuple>

<tuple name="sip:user1_public2@home1.net">
  <status> <value>open</value> </status>
  <detail>automatically by sip:user1_public1@home1.net</detail>
</tuple>
```

Afterwards the S-CSCF shall send the generated NOTIFY request on the dialog and await a 2xx response.



CR-Form-v5

## CHANGE REQUEST

⌘ **24.229** **CR** **080** ⌘ rev **3** ⌘ Current version: **5.0.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Clarification of GPRS aspects		
<b>Source:</b>	⌘ Nokia		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 2002-05-16
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ REL-5
	<i>Use <u>one</u> of the following categories:</i> <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 TR 21.900.		<i>Use <u>one</u> of the following releases:</i> <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>Reason for change:</b>	⌘ The description of the GPRS aspects are incomplete.		
<b>Summary of change:</b>	⌘ Clarification has been added on the activation of PDP Context that carries IM CN subsystem signaling. Furthermore, clarifications have been added on the activation of PDP Contexts that carry media components. These additions align the appropriate sections of 24.229 with the corresponding SA2 decisions on the relation of PDP Contexts and media components.		
<b>Consequences if not approved:</b>	⌘ The descriptions of GPRS-related aspects remain unclear and incomplete.		

<b>Clauses affected:</b>	⌘		
<b>Other specs affected:</b>	<input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> 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/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.htm). Below is a brief summary:

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



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

\*\*\*\*\* FIRST MODIFICATION \*\*\*\*\*

## 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".
- [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".
- [10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".
- [10A] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".
- [10B] 3GPP TS 29.207: " Policy control over Go interface".
- [11] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".
- [12] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx Interface; Signalling flows and message contents".
- [13] 3GPP TS 33.102: "3G Security; Security architecture".
- [14] 3GPP TS 33.203: "Access security for IP based services".
- [15] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".
- [16] RFC 2806: "URLs for Telephone Calls".
- [17] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".
- [18] RFC 2916: "E.164 number and DNS".
- [19] RFC 2976 (October 2000): "The SIP INFO method".
- [20] draft-ietf-sip-rfc2543bis-07 (January 2002): "SIP: Session Initiation Protocol".

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

[21] draft-ietf-sip-100rel-05 (February 2002): "Reliability of provisional responses in SIP".

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

[22] draft-sip-manyfolks- resource-03 (November 2001): "Integration of resource management and SIP".

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

[23] draft-ietf-sip-events-02.txt (February 2002): "SIP-Specific Event Notification".

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

[24] draft-ietf-sip-callerprefs-05 (November 2001): "SIP caller preferences and callee capabilities".

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

[25] draft-ietf-sip-refer-02 (October 2001): "The REFER method".

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

[26] draft-ietf-sip-session-timer-08 (October 2001): "The SIP session timer".

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

[27] draft- sip-privacy-03 (November 2001): "SIP extensions for caller identity and privacy".

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

[28] draft- sip-state-02 (August 2001): "SIP extensions for supporting distributed call state".

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

[29] draft- sip-call-auth-05~~3~~ (November 200~~2~~4): "SIP extensions for media authorization".

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

[30] draft-ietf-mmusic-sdp-new-04 (November 2001): "SDP: Session Description Protocol".

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

\*\*\*\*\* SECOND MODIFICATION \*\*\*\*\*

## 9 GPRS aspects when connected to the IM CN subsystem

### 9.1 Introduction

A UE accessing the IM CN subsystem, and the IM CN subsystem itself, utilises 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 [F510A] and 3GPP TS 29.207 [10B].

## 9.2 Procedures at the UE

### 9.2.1 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]. 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. This PDP context can be either a primary or a secondary PDP context;

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 within the Protocol Configuration Options IE at PDP Context activation. The UE may also use this PDP context for DNS and DHCP signalling according to the static packet filters described in 3GPP TS 29.207 [10B].

#### 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 within the Protocol Configuration Options IE.

NOTE1: A general purpose PDP Context is completely IM CN subsystem-unaware, and as such, it does not have any IM CN subsystem-specific mechanisms applied to it.

NOTE2: 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[10B] and the media component is not mandated by the P-CSCF to be carried in a separate PDP Context.

Editor's note: Actual APN values for IMS are yet not determined.

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

The methods for P-CSCF discovery are:

#### I. Employ DHCP and if needed DNS 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 when activating the PDP context.

If the GGSN provides the UE with a list of P-CSCF IPv6 addresses, 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 coding of the Protocol Configuration Options IE is described in 3GPP TS 24.008 [8].

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 2543bis [20]. 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 in the PDP context activation 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.

## 9.2.2 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.

## 9.2.3 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.

## 9.2.4 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 [15] shall apply while the UE is connected to the IM CN subsystem.

## 9.2.5 PDP contexts for media

During establishment of a session, the UE establishes data streams(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.

The P-CSCF shall indicate to the UE in SIP/SDP if a separate PDP Context is required for a media component as per procedures defined in TS 23.228 [7]. The UE shall establish an additional PDP context for a media component if so indicated by the P-CSCF.

The UE shall 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 by inserting it within the Traffic Flow Template IE at PDP Context activation/modification..

In order to identify to the GGSN which flow(s) (identified by m-lines within the SDP) are to be transferred within a particular PDP context, the UE shall set the flow identifier(s) within the Traffic Flow Template IE at PDP Context activation/modification. Detailed description of how the flow identifiers are constructed is provided in TS 29.207 [10B].

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

## CHANGE REQUEST

⌘ **24.229 CR 081** ⌘ rev **-2** ⌘ Current version: **5.0.0** ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Introduction of Subscription Locator Function Interrogation at I-CSCF in 24.229		
<b>Source:</b>	⌘ Orange France		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 29-04-2002
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ REL-5
	<i>Use one of the following categories:</i> <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 TR 21.900.		<i>Use one of the following releases:</i> <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>Reason for change:</b>	⌘ Subscription Locator Function has been introduced in stage 2 specification TS23.228 and in TS29.228 so that the HSS handling the subscription of a user can be found when there are several HSS in the Home network. This needs to be reflected in TS24.229.  This CR covers I-CSCF case.  The S-CSCF modifications are included in CR060rev4 (Tdoc N1-021109)
<b>Summary of change:</b>	⌘ <ul style="list-style-type: none"> <li>Update title of 29.228</li> <li>Add definition of SLF according to TS23.002 and TS23.228</li> <li>Add SLF in the list of abbreviations</li> <li>Add query of the SLF from I-CSCF during Registration procedure if there are several HSS in the Home network</li> <li>Add abnormal case where the I-CSCF does not receive answer to its SLF query during registration procedure.</li> <li>For Further initial requests at I-CSCF, same changes apply as for Registration procedure at I-CSCF (previous two bullets)</li> </ul>
<b>Consequences if not approved:</b>	⌘ Misalignement with stage 2 specifications

<b>Clauses affected:</b>	⌘ 2, 3.1, 3.2, 5.3.1.2, 5.3.1.3, 5.3.2.1, 5.3.2.2		
<b>Other specs affected:</b>	⌘ <input type="checkbox"/> Other core specifications ⌘ <input type="checkbox"/> Test specifications ⌘ <input type="checkbox"/> 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/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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.

## XXXXXXXXXXXXXXXXXXXXXXXXXXXX NEXT CHANGES XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

---

## 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".
- [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".
- [10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".
- [11] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".
- [12] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".
- [13] 3GPP TS 33.102: "3G Security; Security architecture".
- [14] 3GPP TS 33.203: "Access security for IP based services".
- [15] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".
- [16] RFC 2806: "URLs for Telephone Calls".
- [17] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".
- [18] RFC 2916: "E.164 number and DNS".
- [19] RFC 2976 (October 2000): "The SIP INFO method".
- [20] draft-ietf-sip-rfc2543bis-07 (January 2002): "SIP: Session Initiation Protocol".

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

- [21] draft-ietf-sip-100rel-05 (February 2002): "Reliability of provisional responses in SIP".



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

[22] draft-sip-manyfolks- resource-03 (November 2001): "Integration of resource management and SIP".

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

[23] draft-ietf-sip-events-02.txt (February 2002): "SIP-Specific Event Notification".

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

[24] draft-ietf-sip-callerprefs-05 (November 2001): "SIP caller preferences and callee capabilities".

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

[25] draft-ietf-sip-refer-02 (October 2001): "The REFER method".

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

[26] draft-ietf-sip-session-timer-08 (October 2001): "The SIP session timer".

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

[27] draft- sip-privacy-03 (November 2001): "SIP extensions for caller identity and privacy".

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

[28] draft- sip-state-02 (August 2001): "SIP extensions for supporting distributed call state".

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

[29] draft- sip-call-auth-03 (November 2001): "SIP extensions for media authorization".

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

[30] draft-ietf-mmusic-sdp-new-04 (November 2001): "SDP: Session Description Protocol".

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



XXXXXXXXXXXXXXXXXXXXXXXXXXXXX **NEXT CHANGES** XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

---

## 3 Definitions and abbreviations

### 3.1 Definitions

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

**Header:**

Editor's note: To be provided.

**Option-tag:** unique identifiers used to designate new options in SIP  
These tags are used in Require, Supported and Unsupported header fields.

Editor's note: Text extracted from RFC2543bis, but not specified as a definition.

**Redirect server:** a server that accepts a SIP request, maps the address into zero or more new addresses and returns these addresses to the client  
Unlike a proxy server, it does not initiate its own SIP request. Unlike a user agent server , it does not accept calls.

Editor's note: Previous version of this definition was in the bis draft, but has now been removed. Requires further study as to whether there is a more preferred term.

**Status-code:** a 3-digit integer result code that indicates the outcome of the attempt to understand and satisfy the request

Editor's note: Text extracted from RFC2543bis, but not specified as a definition.

For the purposes of the present document, the following terms and definitions given in RFC 2543bis [20] (*Editor's note – working title*) apply.

**Client**  
**Dialog**  
**Method**  
**Proxy, proxy server**  
**Registrar**  
**Server**  
**Session**  
**(SIP) transaction**  
**Stateful proxy**  
**Stateless proxy**  
**User agent client (UAC)**  
**User agent server (UAS)**  
**User agent (UA)**

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

**Breakout Gateway Control Function (BGCF)**  
**Call Session Control Function (CSCF)**  
**Media Gateway Control Function (MGCF)**  
**Media Resource Function Controller (MRFC)**  
**Subscription Locator Function (SLF)**

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

**Interrogating-CSCF (I-CSCF)**  
**Private user identity**  
**Proxy-CSCF (P-CSCF)**  
**Public user identity**  
**Serving-CSCF (S-CSCF)**

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

**User Equipment (UE)**

## 3.2 Abbreviations

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

1xx	A status-code in the range 101 through 199, and excluding 100
2xx	A status-code in the range 200 through 299
AS	Application Server
AUTN	Authentication TokeN
BGCF	Breakout Gateway Control Function
c	conditional
CK	Ciphering Key
CN	Core Network
CSCF	Call Session Control Function
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
i	irrelevant
I-CSCF	Interrogating CSCF



- 3) forward the REGISTER request to the indicated S-CSCF.

If the user registration status query response from the HSS includes a list of capabilities, the I-CSCF shall:

- 1) select a S-CSCF that fulfils the indicated mandatory capabilities – if more than one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities;
- 2) replace the Request-URI of the received REGISTER request with the URI of the S-CSCF;
- 3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 4) forward the REGISTER request to the selected S-CSCF.

When the I-CSCF receives a 2xx response to a REGISTER request, the I-CSCF shall proxy the 2xx response to the P-CSCF.

### 5.3.1.3 Abnormal cases

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 403 (Forbidden) response to the UE.

If the HSS sends a negative response to the user registration status query request, the I-CSCF shall send back a 403 Forbidden response.

If the user registration status query procedure cannot be completed, e.g. due to time-out or incorrect information from the HSS, the I-CSCF shall send back a 480 Temporarily Unavailable response to the UE.

If a selected S-CSCF:

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

the I-CSCF shall select a new S-CSCF as described in subclause 5.3.1.2, based on the capabilities indicated from the HSS. The newly selected S-CSCF shall not be one of any S-CSCFs selected previously during this same registration procedure.

If the I-CSCF cannot select a S-CSCF which fulfils the mandatory capabilities indicated by the HSS, the I-CSCF shall send back a 600 Busy Everywhere response to the user.

When the I-CSCF receives a 420 Bad Extension response to a REGISTER request, and the Unsupported header contains the value path, the I-CSCF shall take OA&M actions to indicate an error. If the algorithm to select the S-CSCF in 1. above enables an alternative S-CSCF to be selected, then the I-CSCF shall repeat steps 1 through 5 to this new S-CSCF. If no alternative S-CSCF can be selected, the I-CSCF shall proxy the 420 Bad Extension response. In all other cases, the I-CSCF shall proxy the 420 Bad Extension response.

## 5.3.2 Further initial requests

### 5.3.2.1 Normal procedures

The I-CSCF may behave as a stateful proxy for further initial requests.

When the I-CSCF receives an initial request, not containing a Route header, the I-CSCF shall start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [12] for the called user, indicated in the Request-URI.

Prior to performing the user location query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to have to know the HSS name in which the subscriber's data can be found. To obtain the correct HSS name, the I-CSCF may query the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [12].

Upon successful user location query, the I-CSCF shall:

- 1) insert the URL received from the HSS as the topmost Route header;

- 2) store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body. If no <icid> XML element was found, then create a new, globally unique value for the <icid> XML element and insert it into the message body;
- 3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 4) forward the request based on the topmost Route header.

When the I-CSCF receives an initial request containing a Route header, the I-CSCF shall:

- remove its own SIP URL from the topmost Route header;
- apply the procedures as described in subclause 5.3.3; and
- forward the request based on the topmost Route header if present, or based on the Request-URI, in case no topmost Route header is available.

NOTE: In accordance with SIP the I-CSCF can add its own routeable SIP URL to the top of the Record-Route header to any request, independently of whether it is an initial request, or whether topology hiding is performed. The P-CSCF will ignore any Record-Route header that is not in the initial request of a dialog.

### 5.3.2.2 Abnormal cases

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 404 (Not Found) response to the UE.

If the HSS sends a negative response to the user location query, the I-CSCF shall send back a 404 Not Found response.

Editor's Note: The procedures for selection of a default S-CSCF are ffs.

If the I-CSCF receives a CANCEL request and if the I-CSCF finds an internal state indicating a pending Cx transaction with the HSS, the I-CSCF:

- shall answer the CANCEL with a 200 OK;
- shall answer the original request with a 487 Request Terminated; and
- shall silently discard the later arriving (pending) Cx answer message from the HSS.

3GPP TSG-CN1 Meeting #24  
 Budapest, Hungary, 13. – 17. May 2002

Tdoc N1-021433

CR-Form-v5	
<b>CHANGE REQUEST</b>	
⌘ <b>24.229 CR 082</b> ⌘ rev <b>1</b> ⌘	Current version: <b>5.0.0</b> ⌘

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

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Introduction of Visited_Network_ID p-header		
<b>Source:</b>	⌘ Hutchison 3G		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 14 <sup>th</sup> May 2002
<b>Category:</b>	⌘ <b>C</b>	<b>Release:</b>	⌘ REL-5
	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)

<b>Reason for change:</b>	⌘ The current version of 24.229 contains text in the XML body to support visited network identifier, but this is not used anywhere in the procedure text.  It has also been decided that this functionality will be supported via a SIP p-header to be defined in IETF.
<b>Summary of change:</b>	⌘ <u>Rev 1</u> Modified so that header is sent only in REGISTER messages, and not in other requests or responses.  Changes related to S-CSCF are removed as no specified S-CSCF action is required.  New clause 7.2.x and subclauses are included to define the syntax and usage.  <u>Rev 0</u> The procedures at the P-CSCF, and S-CSCF are modified to define when the P-Visited-Network-ID header is inserted or removed into a SIP request.  The XML visited-network-id element and associated description are deleted.
<b>Consequences if not approved:</b>	⌘ No definition of the use of the visited network identifier will be defined in the specification. Not possible to check the existence of roaming agreements.

<b>Clauses affected:</b>	⌘ 2, 5.2.2, 7.2.x (new), 7.6.2, 7.6.3		
<b>Other specs affected:</b>	⌘ <input checked="" type="checkbox"/> Other core specifications	⌘ 24.228	
	<input type="checkbox"/> Test specifications		
	<input type="checkbox"/> O&M Specifications		
<b>Other comments:</b>	⌘ The call flows in 24.228 need to be updated to reflect the use of this p-header.  Requires CR060 to be accepted to be complete – the S-CSCF actions are		

defined there.

### How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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.

---

## 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".
- [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".
- [10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".
- [11] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".
- [12] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx Interface; Signalling flows and message contents".
- [13] 3GPP TS 33.102: "3G Security; Security architecture".
- [14] 3GPP TS 33.203: "Access security for IP based services".
- [15] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".
- [16] RFC 2806: "URLs for Telephone Calls".
- [17] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".
- [18] RFC 2916: "E.164 number and DNS".
- [19] RFC 2976 (October 2000): "The SIP INFO method".
- [20] draft-ietf-sip-rfc2543bis-07 (January 2002): "SIP: Session Initiation Protocol".

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

- [21] draft-ietf-sip-100rel-05 (February 2002): "Reliability of provisional responses in SIP".

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



[22] draft-sip-manyfolks-resource-03 (November 2001): "Integration of resource management and SIP".

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

[23] draft-ietf-sip-events-02.txt (February 2002): "SIP-Specific Event Notification".

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

[24] draft-ietf-sip-callerprefs-05 (November 2001): "SIP caller preferences and callee capabilities".

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

[25] draft-ietf-sip-refer-02 (October 2001): "The REFER method".

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

[26] draft-ietf-sip-session-timer-08 (October 2001): "The SIP session timer".

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

[27] draft-sip-privacy-03 (November 2001): "SIP extensions for caller identity and privacy".

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

[28] draft-sip-state-02 (August 2001): "SIP extensions for supporting distributed call state".


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

[29] draft-sip-call-auth-03 (November 2001): "SIP extensions for media authorization".

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

[30] draft-ietf-mmusic-sdp-new-04 (November 2001): "SDP: Session Description Protocol".

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

 [draft-garcia-sip-visited-network-id-00 \(March 2002\): " Private SIP extension for Visited Network Identifier "](#).

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

## 5.2 Procedures at the P-CSCF

### 5.2.1 General

The P-CSCF shall support use of the Path header.

NOTE: The Path header is only applicable to the REGISTER request and its 200 OK response.

### 5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE that pertains to a given public user identity, the P-CSCF shall:

- insert a Path header in the request. The P-CSCF shall include in the Path header an entry containing the SIP URL identifying the P-CSCF;
- insert a Require header and a Proxy-Require header both containing the option tag "path";
- if the REGISTER request was received with a valid integrity check, add information to the REGISTER request to indicate that the REGISTER request was received with a valid integrity check; and

**Editor's Note : The exact mechanism for this is FFS.**

- [insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network.](#)
- determine the I-CSCF of the home network and forward the request to that I-CSCF.

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

- 1) remove its SIP URL from the list of Path headers, reverses the order of the list and save the resulting list of Path headers. This list shall be stored during the entire registration period of the respective public user identity. This list shall be used to preload the routeing information into the initial requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing Path headers with the new list;
- 2) associate the Path header information with the registered public user identity;
- 3) remove the list of Path headers and "path" option-tags from the 200 OK response before forwarding the response to the UE.

When the P-CSCF receives a 401 Unauthorized response to a REGISTER request, the P-CSCF shall remove and store the CK and IK values contained in the 401 Unauthorized response. The 401 Unauthorized response shall be forwarded to the UE if and only if the CK and IK have been removed.

**Editor's Note: The P-CSCF behaviour when 3xx or 4xx responses other than 401 Unauthorized are received is FFS.**

**Editor's Note: The text above assumes that public user identities are registered one by one. Public user identity might need to be changed to Service Profile in the case when public user identities can be implicitly registered.**

NOTE: The P-CSCF will maintain two Route lists. The first Route list - created during the registration procedure - is used only to pre-load the routeing information into the initial INVITE request that originated at the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

When the P-CSCF receives a 420 Bad Extension response to the above REGISTER request, the P-CSCF shall check the value of the Unsupported header field. When the value of the Unsupported header field is path, the P-CSCF shall take

OA&M actions to indicate an error, in addition to passing on the 420 response to the UE. In all other cases, the P-CSCF shall proxy the 420 Bad Extension response.

---

## 7 Extensions within the present document

### 7.1 SIP methods defined within the present document

There are no SIP methods defined within the present document over and above those defined in the referenced IETF specifications.

### 7.2 SIP headers defined within the present document

#### 7.2.1 Path header

##### 7.2.1.1 Introduction

Path header is a mechanism whereby a P-CSCF, I-CSCFs, and S-CSCF can request to be on a signalling path for the initial INVITE exchanged between the UE and the S-CSCF. The path-establishment procedure is originated by the P-CSCF during the registration process. The procedure is performed during the initial registration of each public user identity and all subsequent reregistrations. The list of Path headers obtained by a reregistration overwrites the existing list of Path headers at the S-CSCF. Each reregistration of the same public user identity may result in new list of Path headers. The P-CSCF uses the list of Path headers to construct a list of Route headers. When initiating a call pertaining to a given public user identity, the list of Route headers will be pre-loaded into the initial INVITE request.. If a CSCF wants to receive subsequent requests, it will insert its own name to the Record Route header of the initial INVITE request. Once on the route, a CSCF remains on the route for the duration of the call. The path learned while reregistering during an active call does not affect the existing call, since the routing path for the respective call has already been established. The list of Path headers is not forwarded to the UE.

##### 7.2.1.2 Syntax

The Path header field has the syntax described in table 7.1.

**Table 7.1: Syntax of path header**

```
Path = "Path" ":" l#(name-addr *(";"rr-param))
rr-param = generic-param
```

##### 7.2.1.3 Operation

The operation of this header is described in clause 5.

### 7.2.2 P-Called-Party-ID header

#### 7.2.2.1 Introduction

The P-Called-Party-ID header is the mechanism whereby the terminating UE learns the dialled public user identity that triggered the current session initiation.

The S-CSCF inserts the header in all terminating INVITE and reINVITE requests. The header is not used in any other request or response.

### 7.2.2.2 Syntax

The P-Called-Party-ID header field has the syntax described in table 7.2.

**Table 7.2: Syntax of P-Called-Party-ID header**

```
P-Called-Party-ID = "P-Called-Party-ID" HCOLON 1#
                    (name-addr *( SEMI p-cdpid-param))

p-cdpid-param = generic-param
```

Table 7.3 is an extension of tables 2 and 3 in RFC 2543bis [20] and table in subclause 7.5 in the SIP-specific event notification [23].

**Table 7.3: P-Called-Party-ID header**

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG	PRA	SUB	NOT
P-Called-Party-ID	R	am	-	-	-	o	-	-	-	-	-

### 7.2.2.3 Operation

The operation of this header is described in subclause 5.4.3.2.

## 7.2.x P-Visited-Network-ID header

### 7.2.x.1 Introduction

The P-Visited-Network-ID header is used to allow the home network (e.g. the HSS) to discover, during the registration procedures, the network(s), other than the home network, that are utilised by the user. This allows the registration to be processed based on this, e.g. actions can be taken that are dependent on the roaming agreements between networks.

### 7.2.x.2 Syntax

The P-Visited-Network-ID header field has the syntax described in draft-garcia-sip-visited-network-id-00 ref [X].

### 7.2.x.3 Operation

The header is inserted by the P-CSCF in every REGISTER request the UE sends. The I-CSCF sends the contents of the header to the HSS.

## 7.6 3GPP IM CN subsystem XML body, version 1

### 7.6.1 General

This subclause describes the Document Type Definition that is applicable for the 3GPP IM CN Subsystem XML body.

Any SIP User Agent or proxy may insert or remove the 3GPP IM CN subsystem XML body or parts of it, as required, in any SIP message. The <icid> XML element is an exception to this rule; it may only be removed by the P-CSCF. The 3GPP IM CN subsystem XML body shall not be forwarded outside a 3GPP network.

The associated MIME type with the 3GPP IMX XML body is "application/3gpp-ims+xml".

### 7.6.2 Document Type Definition

```

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

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

  <!ELEMENT ims-3gpp (vnid?, cell-id?,
    original-dialog-id?, destination-public-user-id?,
    access?, charging-vector?, service-info?)>
  <!ATTLIST ims-3gpp version CDATA #REQUIRED>

  <!-- vnid element: Visited network identity -->
  <!ELEMENT vnid (#PCDATA)>

  <!-- cell-id element: The Cell-Global-ID -->
  <!ELEMENT cell-id (mcc, mnc, lac, ci)>
  <!ELEMENT mcc (#PCDATA)>
  <!ELEMENT mnc (#PCDATA)>
  <!ELEMENT lac (#PCDATA)>
  <!ELEMENT ci (#PCDATA)>
  <!ATTLIST cell-id rat (utran | geran) #REQUIRED>

  <!-- original-dialog-id: original dialog ID -->
  <!ELEMENT original-dialog-id (od-from, od-to, od-call-id)>
  <!ELEMENT od-from (#PCDATA)>
  <!ELEMENT od-to (#PCDATA)>
  <!ELEMENT od-call-id (#PCDATA)>

  <!-- public-user-id: public user ID -->
  <!ELEMENT destination-public-user-id (#PCDATA)>

  <!-- access: the type of access network -->
  <!ELEMENT access (access-type, technology?)>
  <!ELEMENT access-type (gprs | wlan | fixed | (#PCDATA))>
  <!ELEMENT technology (utran | geran | 802.11a |
    802.11b | sat | adsl | (#PCDATA))>

  <!-- charging-vector element: Charging Vector -->
  <!ELEMENT charging-vector (icid, gprs-charging-id?)>

  <!-- icid element: IMS charging identifier -->
  <!ELEMENT icid (#PCDATA)>
  <!-- gprs-charging-id element: GPRS charging identifiers -->
  <!ELEMENT gprs-charging-id (ggsn, pdp-info+)>
  <!ELEMENT ggsn (#PCDATA)>
  <!ELEMENT pdp-info (pdp-index, pdp-id)>
  <!ELEMENT pdp-index (#PCDATA)>
  <!ELEMENT pdp-id (#PCDATA)>

  <!-- 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>
```

### 7.6.3 DTD description

This section describes the elements of the 3GPP IMS Document Type Definition.

<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.

~~<vnid>: Visited network identifier. Optional element that describes the P-CSCF network name. The vnid value is a string of characters that identifies the P-CSCF network at the user's network home.~~

<cell-id>: This element describes the identity of the cell that is serving the user.

The <cell-id> element contains the <ran> attribute that identifies the coding of the cell-id, according to whether the cell-id was received from the GERAN or UTRAN.

The <cell-id> element comprises four children elements: <mcc>, <mnc>, <lac> and <ci>. They represent, respectively, the Mobile Country Code, Mobile Network Code, Location Area Code and Cell Identity, as described in [3].

<original-dialog-id>: The original dialog, as received by the S-CSCF. This element helps the S-CSCF to correlate dialogues when the Application Server is behaving as a B2BUA, and therefore, modifies then dialogue.

The original-dialog-id element comprises three children elements: <od-from>, <od-to>, <od-call-id>. Their values contain, respectively, a copy of the From, To and Call-ID header values as received in the SIP message at the S-CSCF.

<destination-public-user-id>: The destination public-user-id URL of the current session.

<access>: The access element, if present, identifies the access that the UE is utilized to connect to the network. The element contains two children elements: <ant> and <technology>.

The <access-type> child element describes the access type. The predefined values are:

- gprs: the user is accessing the network through a GRPS access;
- wlan: the user is accessing the network through a wireless local area network;
- fixed: the user is accessing the network through a fixed access.

The <technology> child element, if present, describes the access technology. The pre-defined values are:

- utran: UTRAN, as defined in [3];
- geran: GERAN, as defined in [3];
- 802.11a: wireless local area network according to the 802.11a technology;
- 802.11b: wireless local area network according to the 802.11b technology;
- sat: satellite access;
- adsl: asymmetric digital subscriber line.

<charging-vector>: the charging-vector element, if present, identifies charging correlation information. The element contains two children elements: <icid> and <gprs-charging-id>.

The <icid> child element contains an IMS charging identifier that is globally unique and is associated with the end-to-end session.

The <gprs-charging-id> child element, if present, contains GPRS charging identifiers comprised of the following: <ggsn> and <pdp-info>:

- <ggsn>: identifier of the GGSN;
- <pdp-info>: one or more instances of information for a PDP context, which is comprised of two children elements: <pdp-index> and <pdp-id>:
  - <pdp-index>: relative index of PDP context as it correlates to a media stream in the SDP;
  - <pdp-id>: unique identifier of the PDP context from the GGSN.

<service-info>: the transparent element received from the HSS for a particular Application Server 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.