3GPP TSG CN Plenary Meeting #17 **NP-020378**
4th - 6th September 2002. Biarritz, France.

Source: **TSG CN WG 1**

Title: **CRs to Rel-5 on Work Item IMS-CCR towards 24.229,- pack 4**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **9** CRs on **Rel-5 to** Work Item **"IMS-CCR"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #17 for approval.

Spec	CR #	Rev	CAT	Rel	Tdoc Title	Meeting	TDoc #	C_Version
24.229	178		F	Rel-5	Error cases for PDP context modification	N1-25	N1-021679	5.1.0
24.229	183	1	F	Rel-5	Incorporation of draft-ietf-sip-sec-agree-04.txt	N1-25	N1-021791	5.1.0
24.229	185	1	F	Rel-5	User Initiated De-registration	N1-25	N1-021787	5.1.0
24.229	186	1	F	Rel-5	Mobile initiated de-registration	N1-25	N1-021788	5.1.0
24.229	187	1	F	Rel-5	CallID of REGISTER requests	N1-25	N1-021786	5.1.0
24.229	188	1	F	Rel-5	Correction to the I-CSCF routing procedures	N1-25	N1-021803	5.1.0
24.229	189	1	F	Rel-5	Registration procedures at P-CSCF	N1-25	N1-021793	5.1.0
24.229	192	1	F	Rel-5	Corrections related to the P-Access-Network-Info header	N1-25	N1-021827	5.1.0
24.229	194	1	F	Rel-5	Chapter to decribe the registration event	N1-25	N1-021794	5.1.0

3GPP TSG-CN1 Meeting #25 ***Tdoc N1-021679***
Helsinki, Finland, 29 July – 2 August

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **178** ⌘ **rev** **-** ⌘ Current version: **5.1.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Error cases for PDP context modification
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	22/07/2002
Category:	⌘	**F**
Release:	⌘	REL-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change:	⌘	Description of actions within the UE in case the PDP context used for SIP signalling is modified.
Summary of change:	⌘	As the PCO IE is included in the PDP context modification procedure, actions within the UE must be specified in order to avoid faulty behaviour within the UE. Modification of a PDP context from IMS specific to general-purpose or vice versa and reception of new P-CSCF addresses shall not be allowed by the UE.
Consequences if not approved:	⌘	Unwanted behaviour in the UE due to PDP context modification may occur.

Clauses affected:	⌘	New clause 9.2.1A

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

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

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

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;

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 [12];

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;

NOTE 1: 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.

NOTE 2: A general purpose PDP Context may carry both IM CN subsystem signaling and media, in case the media does not need to be authorized by Service Based Local Policy mechanisms defined in 3GPP TS 29.207 [12] and the media component is not mandated by the P-CSCF to be carried in a separate PDP Context.

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

The methods for P-CSCF discovery are:

I. Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) draft-ietf-dhc-dhcpv6 [40], the DHCPv6 options for SIP servers draft-ietf-sip-dhcpv6 [41] 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 of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

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

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

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

9.2.1A Modification of a PDP context used for SIP signalling

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

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

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 [20] 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 3GPP 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 authorisation 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 3GPP TS 29.207 [12].

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

3GPP TSG-CN1 Meeting #25
Helsinki, Finland, 29 July to 2 Aug 2002

Tdoc ⌘ N1-02178610

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **187** ⌘ **rev** **1** ⌘ Current version: **5.1.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	CallID of REGISTER requests
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	22/07/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The SIP RFC allows subsequent REGISTERs to be sent with the same or different CallIDs. In 3GPP the REGISTER carrying RES must be sent with the same CallID as the 401 which carried the challenge.
Summary of change:	⌘	Mandate that the UE will send the REGISTER carrying RES with the same CallID which was used by the 401 which carried the challenge
Consequences if not approved:	⌘	Security hole. No way of correctly applying the AKA mechanism.

Clauses affected:	⌘	5.1.1.5.1

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments:	⌘	

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

1. Introduction

The SIP RFC says: "All registrations from a UAC SHOULD use the same Call-ID header field value for registrations sent to a particular registrar. "

The above text allows consecutive REGISTER requests to be sent with different CallIDs. Consider the following scenario:

1. A fake user sends a REGISTER request to the network, including IMPI1 (CallIDx)

2. The genuine user sends a REGISTER request to the network, including IMPI1 (CallIDy)

3. The S-CSCF challenges both REGISTER requests (this is the only way to avoid DoS). This is allowed by the current text in 24.229: "The S-CSCF need not challenge an unprotected REGISTER request for a private user identity that already has a registration in process"

4. The genuine user responds to the challenge with a protected REGISTER (CallIDz). In this case the registrar does not know to which challenge the response relates. The only way would be to compare RES with both XRES1 and XRES2, but that is not allowed by the AKA mechanism.

It is therefore proposed to mandate in the UE that a REGISTER request carrying the RES need to be sent with the same CallID as the 401 that carried the challenge was received with.

It is further proposed to mandate the S-CSCF to only accept protected REGISTERs carrying RES, if the CallID was used previously to send a challenge to the user. The S-CSCF shall only accept protected REGISTERs carrying RES to the last challenge which was sent to the given user.

Proposed Changes

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 [18] 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 to the REGISTER request 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 [19]; 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). The Call-ID of the integrity protected REGISTER request which carries RES must be the same as the Call-ID of the 401 which carried the challenge.

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.

3GPP TSG-??? Meeting #25
Helsinki, Finland, 29 July to 2 Aug 2002

Tdoc ⌘ N1-02178~~708~~

CR-Form-v7

CHANGE REQUEST

⌘	**24.229**	**CR**	~~**CRNum1**~~ **85**	⌘ **rev**	**-1**	⌘	Current version:	**5.1.0**	⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	User Initiated De-registration
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	22/07/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	S-CSCF can only deregister a public identity, if the request for doing so was sent integrity protected.
Summary of change:	⌘	S-CSCF deregisters a public identity if the request was sent integrity protected. Otherwise a 403 will be sent back.
Consequences if not approved:	⌘	Anyone could deregister everyone (full mesh unsecurity :).

Clauses affected:	⌘	5.4.1.4

	Y	N		
Other specs affected: ⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments:	⌘	

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

5.4.1.4 User-initiated deregistration

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

- check whether the P-CSCF included the Integrity-protection parameter into the Authorisation header field set to yes, indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps if the integrity protection parameter is set to yes;

- deregister the public user identity found in the To header field together with the implicitly registered public user identities;

- 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.

Based on operators' policy the S-CSCF can request from HSS to either be kept or cleared as the S-CSCF allocated to this subscriber. In both cases the state of the subscriber identity is stored as unregistered in the HSS and the S-CSCF. Based on HSS decision, the S-CSCF may either keep all or only a part of the user profile or removes it.

If the Authorisation header of the REGISTER request did not contain an Integrity-protection parameter, or the parameter was set to the value 'no', the S-CSCF shall respond to the request with a 403 Forbidden response. The response may contain a warning header with the reason of rejecting the request.

3GPP TSG-CN1 Meeting #25
Helsinki, Finland, 29 July to 2 Aug 2002

Tdoc ⌘ N1-02178809

CR-Form-v7

CHANGE REQUEST

⌘	24.229	CR	~~CRNum~~1 86	⌘	rev	-1	⌘	Current version:	5.1.0	⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Mobile initiated de-registration
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	22/07/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	UEs can only de-register an IMPU if the request is sent integrity protected.
Summary of change:	⌘	Mandate in the UE that a de-registration request has to be sent integrity protected
Consequences if not approved:	⌘	Bad. Everyone could de-register a registered user.

Clauses affected:	⌘	5.1.1.6

Other specs affected: ⌘	Y	N	
		X	Other core specifications
		X	Test specifications
		X	O&M Specifications

⌘

Other comments: ⌘

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

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.

The UE shall also include the P-Access-Network-Info header in the REGISTER request. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

The request shall be sent integrity protected.

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

3GPP TSG-CN1 Meeting #25
Helsinki, Finland, 29 July to 2 Aug 2002

Tdoc ⌘ N1-02179106

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **183** ⌘ **rev** **-1** ⌘ Current version: **5.1.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Incorporation of draft-ietf-sip-sec-agree-04.txt
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	2002-07-22
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The procedures described in the draft are not yet incorporated into the TS
Summary of change:	⌘	Incorporated the necessary procedures
Consequences if not approved:	⌘	Lack of security in IMS

Clauses affected:	⌘	2, 5.1.1.2, 5.1.1.4, 5.1.1.5			
Other specs affected:	⌘	**Y**	**N**		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

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

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 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

[12] 3GPP TS 29.207: "Policy control over Go interface".

[13] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".

[14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[15] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".

[16] 3GPP TS 32.200: "Telecommunication management; Charging management; Charging principles".

[17] 3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia subsystem".

[18] 3GPP TS 33.102: "3G Security; Security architecture".

[19] 3GPP TS 33.203: "Access security for IP based services".

[20] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[21] RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[22] RFC 2806: "URLs for Telephone Calls".

[23] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[24] RFC 2916: "E.164 number and DNS".

[25] RFC 2976 (October 2000): "The SIP INFO method".

[26] RFC 3261 (March 2002): "SIP: Session Initiation Protocol".

[27] RFC 3262 (March 2002): "Reliability of provisional responses in Session Initiation Protocol".

[28] RFC 3265 (March 2002): "Session Initiation Protocol Specific Event Notification".

[29] RFC 3311 (April 2002): "The SIP UPDATE method".

[30] RFC 3312 (May 2002): "Integration of resource management and SIP".

[31] RFC 3313 (February 2002): "SIP extensions for media authorization".

[32] RFC 3320 (March 2002): "Signaling Compression (SigComp)"

[33] RFC 3323 (May 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[34] RFC 3325 (May 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".

[35] RFC 3327 (May 2002): "SIP Extension for Registering Non-Adjacent Contacts".

[36] draft-sparks-sip-refer-split-00 (April 2002): "The REFER method".

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

[37] draft-sparks-sip-mimetypes (April 2002): "Internet Media Type message/sipfrag".

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

[38] draft-willis-scvrtdisco-03 (May 2002): "SIP Extension Header for Service Route Discovery in Private Networks".

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

[39] 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.

[40] 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.

[41] 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.

[42] draft-ietf-sipping-sigcomp-sip-dictionary-00.txt (May 2002): "The SIP/SDP static dictionary for Signaling Compression".

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

[43] draft-beckmann-sip-reg-event-01 (May 2002): "Registration event package".

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

[44] 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.

[45] draft-henrikson-sip-charging-information-01 (May 2002): "Private SIP Extension for Mobile Charging Information".

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

[46] draft-henrikson-sip-original-dialog-id-01 (May 2002): "Private SIP Extension for Original Dialog Identifier".

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

[47] draft-mills-sip-access-network-info-01.txt (April 2002): “SIP Access Network Information header”

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

[48] draft-ietf-sip-sec-agree-04.txt (June 2002): "Security Mechanism Agreement for SIP Sessions"

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

[49] draft-ietf-sip-digest-aka-03.txt (May 2002): " HTTP Digest Authentication Using AKA"

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

5.1.1.2 Initial registration

The UE can register a public user identity at any time that a valid PDP context exists. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

A REGISTER request may be integrity protected using IK, see 3GPP TS 33.203 [19], received in an earlier registration.

The public user identity to be registered can be extracted either from the ISIM application, if present, on the UICC or derived from the USIM, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user. On sending a REGISTER request, the UE shall populate the header fields as follows:

a) the user ID field of the authentication protocol, carried in the Authorization header, shall contain the private user identity;

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; and

e) a Request-URI that contains the SIP URI of the domain name of the home network.

f) insert the Security-Client header field by specifying the security mechanism it supports, the IPSec layer algorithms it supports and the parameters needed for the security association setup. For further details see 3GPP TS 33.203 [19] and draft-ietf-sip-sec-agree [48]

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 (Interval Too Brief) response.

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

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

The UE shall also include the P-Access-Network-Info header in the REGISTER request. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

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 (Interval Too Brief) too brief response to the REGISTER request, the UE shall:

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

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~~ shall be integrity protected using IK, see 3GPP TS 33.203 [19], received in an earlier registration, if ~~possible~~IK is available.

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 REGISTER request.

e) ~~insert~~ the Security-Client header field, by specifying the security mechanism it supports, the IPSec layer algorithms it supports and the parameters needed for the security association setup. For further details see 3GPP TS 33.203 [19] and draft-ietf-sip-sec-agree [48].

NOTE1: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

NOTE2: The security setup mechanism is not used in the way described in draft-ietf-sip-sec-agree [48]. The 401 challenge sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up the security association with the UE during the same registration procedure.

The UE shall also include the P-Access-Network-Info header in the REGISTER request. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

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 UE shall set up the Security Association based on the static list it received in the 401 and its capabilities sent in the Security-Client header in the REGISTER request. The Security Association shall be set up using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE.

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 (Interval Too Brief) response to the REGISTER request, the UE shall:

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

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 [18] 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.

- check the existence of the Security-Server header as described in draft-sip-sec-agree [48]. If the header is not present, a new REGISTER request shall be sent.

In the case that the 401 (Unauthorized) response to the REGISTER request 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 [19]; 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). Instead of the Security-Client header the UE shall insert the Security-Verify header into the request, by mirroring in it the content of the Security-Server header received in the 401.

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 request 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 request 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 request shall contain the AUTS parameter (see 3GPP TS 33.102 [18]).

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.

3GPP TSG-CN1 Meeting #25
Helsinki, Finland, 29 July to 2 Aug 2002

Tdoc ⌘ N1-021791~~1~~3

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **189** ⌘ **rev** **-1** ⌘ Current version: **5.1.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Registration procedures at P-CSCF
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	2002-07-22
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	SA related procedures are not covered yet in the TS.
Summary of change:	⌘	SA related procedures added to the P-CSCF
Consequences if not approved:	⌘	Non-workable IMS

Clauses affected:	⌘	5.2.2; 5.2.5			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

5.2.2 Registration

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

1) insert a Path header in the request including an entry containing:

   - the SIP URL identifying the P-CSCF;

   - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) shall be treated as for the mobile-terminating case. This indication may e.g. be in a Path header parameter, a character string in the user part or be a port number;

2) insert a Supported and a Require header both containing the option tag "path";

3) for the initial REGISTER request for a public user identity create a new, globally unique value for icid, save it locally and insert it into the icid parameter of the P-Charging-Vector header (see subclause 7.2.5). Also include the gprs-charging-info parameter in the P-Charging-Vector header (see subclause 5.2.7.4);

4) insert the parameter "integrity-protected" (described in subclause 7.2A.2) with a value “yes” into the Authorization header field in case the REGISTER request was received integrity protected, otherwise insert the parameter with the value “no”;

5) ~~I~~in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The 'Require: sec-agree' header shall also be removed. If the header is not present, then a suitable 4xx error code shall be sent back.

6) In case the REGISTER request was received integrity protected, then the P-CSCF shall:

   - check the ~~SA~~Security Association which protected the request. If that has a temporary lifetime, then the request shall contain a Security-Verify header. If there is no such header, then a suitable 4xx error code shall be sent back. If there is such header, then compare the content of the Security-Verify header with the local static security list. If those do not match, then there is a potential ~~DoS~~man-in-the-middle attack. The request should be rejected by sending a suitable 4xx error response. If the contents match, then the Security-Verify header together with the 'Require: sec-agree' header shall be removed from the request.

   - If the ~~SA~~Security Association the REGISTER request came is an established one, then a Security-Verify header is not expected to be included. If the header is present, then that shall be removed together with the 'Require: sec-agree' header.

7~~5~~) insert a P-Visited-Network-ID header field, with the value of a pre-provisioned string that identifies the visited network at the home network; and

8~~6~~) determine the I-CSCF of the home network and forward the request to that I-CSCF.

When the P-CSCF receives a 401 (Unauthorized) response to a REGISTER request, the P-CSCF shall:

1) 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

2) insert the Security-Server header in the response, containing the P-CSCF static security list. For further information see 3GPP TS 33.203 [19].

3) set up the Security Association between the UE and the P-CSCF with a temporary lifetime. For further details see 3GPP TS 33.203 [19] and draft-sip-sec-agree [48]. The SIP level lifetime of the Security Association shall be long enough to permit the UE to finalize the registration procedure (bigger than 64*T1). The IPSec level lifetime of the ~~SA~~Security Association shall be set to the maximum.

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

1) save the list of P-Service-Route headers preserving the order. 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 list of P-Service-Route headers with the new list;

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

3) remove any Path and P-Service-Route headers 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;

5) store the default public user identity for use with procedures for the P-Asserted-Identity. The default public user identity is specifically indicated in the Associated-URI header values.

Editor's note: The exact mechanism for indicating this value is for further discussion.

6) ~~When the P-CSCF receives a 200 (OK) response to a REGISTER request, the P-CSCF shall~~ store the values received in the P-Charging-Function-Addresses header.

7) update the SIP level lifetime of the Security Association with the value found in the Expire header.

~~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.~~

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.

The P-CSCF shall delete any ~~SA~~Security Association from the IPSec database when their SIP level lifetime expires.

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:

1) - remove the public user identity found in the To header field, and all the associated public user identities, from the registered public user identities list and all related stored information, and

2) - check if the user has left any other registered public user identity. When all of the public user identities of a user are deregistered, the P-CSCF shall remove the SAs towards that user.

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

5.2.5.2 Network-initiated deregistration

If the P-CSCF:

- has subscribed for the registration-state event package providing registration state information of a certain public identity and public user identities implicitly registered with it; and,

- an incoming NOTIFY request arrives on the dialog which was generated during subscription (as described in subclause 5.2.3) containing the registration state value “closed”, i.e. deregistered, for one or more public user identities;

the P-CSCF shall release all stored information for these public user identities which are indicated with registration state "closed".

The P-CSCF shall check if the user has left any other registered public user identity. When all of the public user identities of a user are deregistered, the P-CSCF shall remove the SAs towards that user.

3GPP TSG-CN WG1 Meeting #25
Helsinki, Finland, 29th July – 2nd August

Tdoc ⌘N1-021794

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **1945** ⌘ **rev** **1** ⌘ Current version: **5.1.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Chapter to decribe the registration event~~Introdcution of a chapter to decribe the registration event~~
Source:	⌘	Siemens AG
Work item code:	⌘	IMS-CCR
Date:	⌘	23/07/02
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change: ⌘ During CN1#24 it was requested that a new chapter should be introduced where the registration state event package should be decsribed and that this chapter shall be referenced whenever refering to this event package.~~ This CR introduces a new chapter and changes all references within other parts of the specification accordingly~~. However, at the last IETF meeting it was decided to move forward with draft-rosenberg-sip-reg instead of draft-beckmann-sip-re-event regarding the registration state event package. Therefore a new chapter is not needed. Instead, this CR aligns 24.229 with the rosenberg draft.

Summary of change: ⌘

1) Replace reference to draft-beckmann-sip-reg-event-01 with draft-rosenberg-sip-reg-00

2) Change of registration state event name to "reg" event

3) Within the Rosenberg draft, the registration state of each contact may be signalled using a state and event parameter, where the state parameter indicates the current state of the contact (active or terminated) and the event parameter describes the reason which triggered the change of state.

Within 3GPP basically 3 states, namely "registered", "deregistered" and "re-authentication needed", need to be indicated.

The following mapping from the states and events as they are described in the rosenberg draft to the "3GPP" registration states is applied:

- The "registered" state is indicated by setting the state parameter of the corresponsing <contact> element to "active" irresepective of the event parameter setting.

		- The "deregistered" state is indicated by setting the state parameter of the corresponding <contact> element to "terminated". In case of network initiated de-registration the event parameter shall be set to "rejected" in order to indicate that the UE should not try to re-register this contact (public user identity). - The "re-authentication needed" state is indicated by setting the state parameter of the corresponding <contact> to "terminated" and the event parameter to "deactivated". 4) The public user identity that has been registered by the UE is indicated in the adress of record (aor) parameter of the <registration> element and the public user identities that belong to the same service profile shall be indicated in the <contact> elements. If the public user identities have automatically been registered the event parameter of those <contact> elements shall be set to "created".~~- Introduction of a new section in chapter 7~~ ~~- Change of references in the UE and P-CSCF procedures~~
Consequences if not approved:	⌘	IETF and 3GPP specifications would not be aligned. After expiration of draft-beckmann-sip-reg-event-01 no documentation of the registration state event package would be available ~~In case the registration state event package is not approved by IETF or aditional restriction/extensions have to be applied for 3GPP needs no place holder exists where to put this information~~

Clauses affected:	⌘	2; 5.1.1.3; 5.1.1.5.2; 5.1.1.7; 5.1.2; 5.1.2.1; 5.2.3; 5.2.4; 5.2.5.2; 5.4.1.5; 5.4.1.6; 5.4.2.1.1; 5.4.2.1.2;~~5.1.1.3; 5.2.3; 7~~				
Other specs affected:	⌘	**Y**	**N**		⌘	
		X		Other core specifications		TS 24.228
				Test specifications		
				O&M Specifications		
Other comments:	⌘					

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

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 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

[12] 3GPP TS 29.207: "Policy control over Go interface".

[13] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".

[14] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents".

[15] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".

[16] 3GPP TS 32.200: "Telecommunication management; Charging management; Charging principles".

[17] 3GPP TS 32.225: "Telecommunication management; Charging management; Charging data description for the IP Multimedia subsystem".

[18] 3GPP TS 33.102: "3G Security; Security architecture".

[19] 3GPP TS 33.203: "Access security for IP based services".

[20] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[21] RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[22] RFC 2806: "URLs for Telephone Calls".

[23] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[24] RFC 2916: "E.164 number and DNS".

[25] RFC 2976 (October 2000): "The SIP INFO method".

[26] RFC 3261 (March 2002): "SIP: Session Initiation Protocol".

[27] RFC 3262 (March 2002): "Reliability of provisional responses in Session Initiation Protocol".

[28] RFC 3265 (March 2002): "Session Initiation Protocol Specific Event Notification".

[29] RFC 3311 (April 2002): "The SIP UPDATE method".

[30] RFC 3312 (May 2002): "Integration of resource management and SIP".

[31] RFC 3313 (February 2002): "SIP extensions for media authorization".

[32] RFC 3320 (March 2002): "Signaling Compression (SigComp)"

[33] RFC 3323 (May 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[34] RFC 3325 (May 2002): "Private Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks".

[35] RFC 3327 (May 2002): "SIP Extension for Registering Non-Adjacent Contacts".

[36] draft-sparks-sip-refer-split-00 (April 2002): "The REFER method".

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

[37] draft-sparks-sip-mimetypes (April 2002): "Internet Media Type message/sipfrag".

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

[38] draft-willis-scvrtdisco-03 (May 2002): "SIP Extension Header for Service Route Discovery in Private Networks".

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

[39] 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.

[40] 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.

[41] 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.

[42] draft-ietf-sipping-sigcomp-sip-dictionary-00.txt (May 2002): "The SIP/SDP static dictionary for Signaling Compression".

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

~~[43] draft-beckmann-sip-reg-event-01 (May 2002): "Registration event package".~~

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

[43] draft-rosenberg-sip-reg-00 (May 2002): "A Session Initiation Protocol (SIP) Event Package for Registrations".

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

[44] 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.

[45] draft-henrikson-sip-charging-information-01 (May 2002): "Private SIP Extension for Mobile Charging Information".

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

[46] draft-henrikson-sip-original-dialog-id-01 (May 2002): "Private SIP Extension for Original Dialog Identifier".

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

[47] draft-mills-sip-access-network-info-01.txt (April 2002): “SIP Access Network Information header”

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

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-statereg event package for the public user identity registered as described in subclause 5.1.1.2 at the users registrar (S-CSCF). The registration-statereg event package is described in draft-rosenberg-sip-reg-00 [43]draft-beckmann-sip-reg-event-01 [43]section 7.8. 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;
- a From header set to a SIP URL that contains a public user identity;
- a To header, set to a SIP URL that contains a public user identity;
- an Event header set to the "registration-statereg" event package;
- an Expires header set to a value higher than the Expires header of the before sent REGISTER request.

The UE shall also include the P-Access-Network-Info header in the SUBSCRIBE request. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

Afterwards it shall send out the so generated SUBSCRIBE request.

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

The UE shall automatically resubscribe to the registration-statereg 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 request, has run out and the public user identity is still registered.

5.1.1.5.2 Network-initiated re-authentication

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the registration-state event package, which contains the registration-state valuethe state parameter set to "terminated" and the event parameter set to "re-authenticateexpireddeactivated" 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.

5.1.1.7 Network-initiated deregistration

Upon receipt of a NOTIFY request 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 parameter set to "closedterminated" and the event parameter "rejected", 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.

5.1.2 Subscription and notification

5.1.2.1 Notification about multiple registered public user identities

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

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

- if a registration state value parameter "openactive", i.e. registered is received for one or more public user identities, the UE shall store the indicated public user identities as registered;

- if a registration state value parameter "closedterminated", i.e. deregistered is received for one or more public user identities, the UE shall store the indicated public user identities as deregistered.

NOTE: There may be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity. Usually these automatically or implicitly registered public user identities belong to the same service profile of the user and they might not be available within the UE, i.e. the UE 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.

5.2.3 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-statereg event package at the users registrar (S-CSCF) as described in draft-beckmann-sip-reg-event-01 [43]. draft-rosenberg-sip-reg-00 [43]section 7.8. 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 the P-CSCF's SIP URL;
- 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-statereg" 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 request, 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 request on the dialog which was generated during subscription to the registration-statereg event package, the P-CSCF shall perform the following actions:

- if a registration state value parameter "openactive", 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 parameter "closedterminated", 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.

5.2.5.2 Network-initiated deregistration

If the P-CSCF:

- has subscribed for the registration-statereg event package providing registration state information of a certain public identity and public user identities implicitly registered with it; and,

- an incoming NOTIFY request arrives on the dialog which was generated during subscription (as described in subclause 5.2.3) containing with the registration state value parameter set to "closedterminated" and the event parameter set to "rejected", i.e. deregistered, for one or more public user identities;

the P-CSCF shall release all stored information for these public user identities which are indicated with registration state parameter set to "closedterminated".

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 the registration state registration events, 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 deregister 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 statereg 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 statereg" 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 the state parameter set to "re-authenticateterminated" and the event parameter set to "expireddeactivated".

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 request.

When generating the NOTIFY request, the S-CSCF shall shorten the validity of subscriber's registration timer to an operator defined value that will allow the user to be re-authenticated. If user fails to reauthenticate while its registration is still valid, 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.

5.4.2 Subscription and notification

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-statereg 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.

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

Notification of the registration state shall affect the non-barred public user identities. The barred public user identities shall never be sent in a NOTIFY message.

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-statereg 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 "registrationreg- state" value;
- in the NOTIFY body, indicate the public user identity that has been registered by the UE within the aor parameter of the <registration> element;
- indicate registrationindicate the public user identities that belong to the same service profile including the one that has been registered by the UE in the <contact> elements; and
- set -state parameter in the <contact> elements to "active""open" for all public user identities which are currently registered; and;
- indicate registrationset -state parameter in the <contact> element to "closedterminated" for all public user identities which are currently deregistered; and
- indicate within the "<note>" information of those public user identities which will be automatically reregistered the "automatically by" information. , followed by t by setting the event parameter to "created". The user identity which will cover the reregistration is indicated in the aor parameter of the <registration> element.he specific public user identity which will cover the reregistration.

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

```
   <?xml version="1.0"?>
   <reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
                 version="0" state="full">
     <registration aor="sip:user1_public1@home1.net" id="as9"
                   state="active">
       <contact id="76" state="active" event="registered"
              >sip:user1_public1@home1.net</contact>
       <contact id="66" state="active" event="created"
              >sip:user1_public2@home1.net</contact>
     </registration>
   </reginfo>
<tuple name="sip:user1_public1@home1.net">
  <status><basic>open</basic><<<</status>
```

```
</tuple>

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

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

7.8 Reg event package

The registration state event package is defined in draft-rosenberg-sip-reg-00 [43].

3GPP TSG-CN1 Meeting #25
Helsinki, Finland, 29 July to 2 Aug 2002

Tdoc ⌘ N1-021803~~711~~

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **188** ⌘ **rev** **-1** ⌘ Current version: **5.1.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Correction to the I-CSCF routing procedures
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	22/07/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The routing procedures at the I-CSCF as described in version 5.1.0 of this TS does not allow for a THIG to encrypt messages which leaves the home network. If however, the home network wishes to do such hiding, the resulting behaviour of the network would not be predictable.
Summary of change:	⌘	A new condition is added. It has to be verified whether the message has to be routed inside the home domain or outside of it.
Consequences if not approved:	⌘	Calls would fail if the home network would like to apply hiding against the external network.
Clauses affected:	⌘	5.3.2.1

	Y	N		
Other specs affected: ⌘		**X**	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

1. Introduction

In 3GPP TS 24.229v5.1.0, section 5.3.2.1 it is said: " When the I-CSCF receives an initial request, that either does not contain a Route header or contains a single Route header pointing to itself, the I-CSCF shall start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [14] for the called user, indicated in the Request-URI. "

The above text eliminates the possibility of routing the request to the boundary of the network for hiding purposes and then the hiding network entity would route it further towards the next network domain.

The I-CSCF may receive a massage in the following situations:

- MO case, message received from the P-CSCF. In this case the Route header would contain the address of the I-CSCF and the address of the S-CSCF (two). Loose routing is performed.
- Both parties are part of the same network. The O-SCSCF will send the message to the I-CSCF for HSS query purposes. The I-CSCF name will be present in the route header. The Request-URI field would point to a user in the same domain.
- I-CSCF receives an incoming message from a n external network. No Route headers present. The Request-URI will point to a user in the same network as the I-CSCF itself. HSS query has to be performed.
- I-CSCF receives an incoming message from the S-CSCF for outgoing hiding purposes. The I-CSCF address is the only one present in the route header. The request URI will point to a user in a different domain than the I-CSCF is part of.
- (error case) The I-CSCF receives a message from an external network and the Request-URI does not point to a user in the same domain as the I-CSCF is part in. Proposal is to route the request based on the Request-URI (to the correct home domain).

The I-CSCF will never need to perform both hiding and HSS query when receiving a message. The following changes are proposed:

Proposed Changes

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, that ~~either~~ does not contain a Route header, ~~or contains a single Route header pointing to itself, and the Request-URI header field points to a domain in which the I-CSCF is part of,~~ the I-CSCF shall start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [14] 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 the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

Upon successful user location query, when the response contains the URL of the assigned S-CSCF, the I-CSCF shall:

1) if present, remove its own SIP URL from the topmost Route header;

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

3) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. If no icid parameter was found, then create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header;

4) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

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

Upon successful user location query, when the response contains information about the required S-CSCF capabilities, the I-CSCF shall:

1) select a S-CSCF according to the method described in 3GPP TS 29.228 [14];

2) insert the URL of the selected S-CSCF as the topmost Route header field value;

3) execute the procedure described in step 2 and 3 in the above paragraph (upon successful user location query, when the response contains the URL of the assigned S-CSCF); and

4) forward the request to the selected S-CSCF.

Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) or 604 (Does not exist anywhere) in the case the user is not a user of the home network.

Upon an unsuccessful user location query when the response from the HSS indicates that the user is not registered and no services are provided for such a user, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) if the user is recognized as a valid user, but is not registered at the moment and it does not have services for unregistered users.

When the I-CSCF receives an initial request, that contains a single Route header pointing to itself, the I-CSCF shall determine from the entry in the Route header whether it needs to do HSS query or hiding. In case HSS query is needed, then the procedures described for the case when there is no Route header present shall be performed. If the I-CSCF determines that hiding must be performed, then the THIG functionality in I-CSCF received an outgoing initial request for which topology hiding has to be applied, and the I-CSCF shall:

1. remove its own SIP URL from the topmost Route header;

2. perform the procedures described in subsection 5.3.3, and

3. route the request based on the Request-URI header field

When the I-CSCF receives an initial request containing more than one Route header, the I-CSCF shall:

1) remove its own SIP URL from the topmost Route header;

2) apply the procedures as described in subclause 5.3.3; and

3) 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.

~~When the I-CSCF receives an initial request, that either does not contain a Route header or contains a single Route header pointing to itself, and the Request-URI header field points to a different domain than the I-CSCF is part of, the I-CSCF shall:~~

~~1) if present, remove its own SIP URL from the topmost Route header;~~

~~2) apply the hiding procedures as described in subclause 5.3.3; and~~

~~3) 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.

When the I-CSCF receives a response to an initial request (e.g. 183 or 2xx), the I-CSCF shall store the values from the P-Charging-Function-Addresses header, if present. If the next hop is outside of the current network, then the I-CSCF shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

3GPP TSG-CN1 Meeting #25 ***Tdoc N1-021827***
Helsinki, Finland, 29 July – 2 August **Revision of N1-021733**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **192** ⌘ **rev** **1** ⌘ Current version: **5.1.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Corrections related to the P-Access-Network-Info header
Source:	⌘	Vodafone
Work item code:	⌘	IMS-CCR
Date:	⌘	18/07/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Some slight alterations to the corresponding internet draft require that similar changes are made in 24.229 in order to align the two. Additionally, other sections of 24.229 need to contain text relating to the P-Access-Network-Info header.
Summary of change:	⌘	P-Access-Network-Info header is added to various sub-clauses and some of the parameters within the header require their name to be changed.
Consequences if not approved:	⌘	

Clauses affected:	⌘	5.1.2A.1, 5.1.2A.2, 5.4.1.4, 5.4.3.2, 5.4.3.3, 5.4.6.1.2, 5.4.6.1.3, 7.2.3.3

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

5.1.2A.1 Mobile-originating case

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

- a public user identity stored in the USIM which has been registered by the user;
- a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implict registration; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

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

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

NOTE 2: It is a matter of network policy as to whether any of the contents of the From header are modified based on any privacy specified by the user either within the UE indication of privacy or by network subscription. Therefore the user could require to include the value "Anonymous" even on requests where privacy is not explicitly requested.

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

The UE shall insert a P-Access-Network-Info header into any request for a dialog, any subsequent request or response within a dialog or any request for a standalone method. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

5.1.2A.2 Mobile-terminating case

The UE can indicate privacy of the P-Asserted-Identity in accordance with RFC 3323 [33].

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

The UE shall insert a P-Access-Network-Info header into any response to a request for a dialog, any subsequent request or response within a dialog or any response to a standalone method. This header shall contain information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2.3).

5.4.1.4 User-initiated deregistration

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

- deregister the public user identity found in the To header field together with the implicitly registered public user identities;
- 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.

Based on operators' policy the S-CSCF can request from HSS to either be kept or cleared as the S-CSCF allocated to this subscriber. In both cases the state of the subscriber identity is stored as unregistered in the HSS and the S-CSCF. Based on HSS decision, the S-CSCF may either keep all or only a part of the user profile or removes it.

5.4.3.2 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:

- determine whether the request contains a barred public user identity in the From or Remote-Party-ID header fields of the request or not. In case any of the said header fields contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. Otherwise, continue with the rest of the steps;

- 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 [22]) to a globally routeable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or an appropriate SIP response shall be sent to the originator;

- check if P-Original-Dialog-ID header is present in 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-tag, od-from-tag and od-call-idparameter values from the P-Original-Dialog-ID header 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 P-Original-Dialog-ID header in the request. If the next hop is not an Application Server, the S-CSCF shall remove the P-Original-Dialog-ID header from the request;

- 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

  - populate the P-Original-Dialog-ID header in the message with the original To tag, From tag and Call-ID headers received in the request. See subclause 7.2.7 for further information on the original dialog identifier;

- store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header. Optionally, the S-CSCF may generate a new, globally unique icid and insert the new value in the icid parameter of the P-Charging-Vector header when forwarding the message. If the S-CSCF creates a new icid, then it is responsible for maintaining the two icid values in the subsequent messaging;

- insert an ioi-originating parameter into the P-Charging-Vector header if the next hop is an AS, I-CSCF or outside of the current network. The ioi-originating parameter shall be set to a value that identifies the sending network. The ioi-terminating parameter shall not be included;

- insert a P-Charging-Function-Addresses header (see subclause 7.2.5) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

- in the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URL contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;

- in the case where the network operator has policy to provide privacy on From headers, and such privacy is required for this dialog, change the From header to "Anonymous". Network policy may also require the removal of the display field;

- 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;

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

- 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 Record-Route header fields and the Contact header from the request in order to release the dialog when needed;

- remove the P-Access-Network-Info header and act upon the contents accordingly; and

- route the request based on SIP routeing procedures.

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

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

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

NOTE 2: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3323 [33].

When the S-CSCF receives a response to the initial request for a dialog, it shall save the necessary Record-Route header fields and the Contact header from the response in order to release the dialog if 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 Contact header from the request in order to release the dialog when needed;

- remove the P-Access-Network-Info header and act upon the contents accordingly; and

- route the request based on the topmost Route header.

When the S-CSCF receives a response to the refresh request for a dialog, it shall save the necessary Record-Route header fields and the Contact header from the response in order to release the dialog if needed.

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;

- remove the P-Access-Network-Info header and act upon the contents accordingly; ~~and~~

- remove the P-access-network-info header and act upon the contents accordingly; and

- route the request based on the topmost Route header.

5.4.3.3 Requests terminated at the served user

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

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

2) check if P-Original-Dialog-ID header is present in 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-tag, od-from-tag and od-call-id parameter values from the P-Original-Dialog-ID header may be used as additional parameters when searching for existing dialogs. The S-CSCF shall determine the next hop using initial filter criteria. If the next hop is another Application Server, the S-CSCF shall retain the P-Original-Dialog-ID header in the message of the request. If the next hop is not an Application Server, the S-CSCF shall remove the P-Original-Dialog-ID header from the request;

3) 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:

a) insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and

b) populate the P-Original-Dialog-ID header in the message with the original To tag, From tag and Call-ID headers received in the request. See subclause 5.4.3.4 for further information on the original dialog identifier;

4) insert a P-Charging-Function-Addresses header (see subclause 7.2.4) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

5) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header;

6) store the value of the ioi-originating parameter received in the P-Charging-Vector header, if present. The ioi-originating parameter identifies the sending network of the request message. The ioi-originating parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS;

7) 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;

8) build the Route header field with the values determined in the previous step;

9) 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;

10) build a Request-URI with the contents of the saved Contact URL determined in the previous step;

11) insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;

12) in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary Record-Route header fields and the Contact header from the request in order to release the dialog when needed; and

13) optionally, apply any privacy required by RFC 3323 [33] to the P-Asserted-Identity header; and

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

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

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

1) execute the procedures described in the steps 1 and 2 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction);

2) if the S-CSCF does not have the user profile, then initiate the S-CSCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informing the HSS that the user is unregistered, but this S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [14];

3) keep the user registration status as unregistered for the duration of the dialog. When the dialog expires, the S-CSCF shall inform appropriately the HSS according to the procedures described in 3GPP TS 29.228 [14];

4) execute the procedure described in step 3 and 4 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

In case that no AS needs to be contacted, then S-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) and terminate these procedures; and

5) execute the procedures described in the steps 5, 6, 11, 12, 13 and 14 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

When the S-CSCF receives a response to the initial request for a dialog (whether the user is registered or not), it shall save the necessary Record-Route header fields and the Contact header field from the response in order to release the dialog if needed. In the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URL contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel-URI; in the case where the network operator has policy to provide privacy on To headers, and such privacy is required for this dialog, change the To header to "Anonymous". Network policy may also require the removal of the display field.

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

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

2) create a Record-Route header containing its own SIP URL and save the Contact header from the refresh request in order to release the dialog when needed; and

~~3) remove the P-Access-Network-Info header, if it is present, and may act upon its contents accordingly; and~~

~~4~~3) forward the request based on the topmost Route header.

When the S-CSCF receives a response to the refresh request for a dialog (whether the user is registered or not), it shall save the necessary Record-Route header fields and the Contact header field from the response in order to release the dialog if needed.

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:

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

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

When the S-CSCF receives a request destined for a barred public user identity, the S-CSCF shall return an appropriate unsuccessful SIP response. This response may be, e.g., a 404 (Not found) or 604 (Does not exist anywhere).

5.4.6.1.2 Mobile-originating case

For a reINVITE request from the UE, when the S-CSCF receives the UPDATE request, the S-CSCF shall store the updated gprs-charging-info parameter from P-Charging-Vector header. The gprs-charging-info parameter shall be retained in the P-Charging-Vector header when the request is forwarded to an AS. However, the gprs-charging-info parameter shall not be included in the P-Charging-Vector header when the UPDATE request is forwarded outside the home network of the S-CSCF.

For a reINVITE request from the UE, the S-CSCF shall also remove the P-Access-Network-Info header and may act upon its contents accordingly.

5.4.6.1.3 Mobile-terminating case

For a reINVITE request destined towards the UE, when the S-CSCF receives the 200 (OK) response (to the INVITE), the S-CSCF shall store the updated gprs-charging-info parameter from the P-Charging-Vector header. The gprs-charging-info parameter shall be retained in the P-Charging-Vector header when the response is forwarded to the AS. However, the gprs-charging-info parameter shall not be included in the P-Charging-Vector header when the 200 (OK) response is forwarded outside the home network of the S-CSCF.

For a 200 (OK) response to an INVITE, the S-CSCF shall also remove the P-Access-Network-Info header and may act upon its contents accordingly.

7.2.3.3 Additional coding rules for P-Access-Network-Info header

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

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

The Cell Global Identity is a concatenation of MCC, MNC, LAC and CI (as described in 3GPP TS23.003). The value of "~~3GPP-~~CGI-3GPP" is therefore coded as a text string as follows:

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

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

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