3GPP TSG CN Plenary Meeting #18 **NP-020564**
4th - 6th December 2002. New Orleans, USA.

Source: **TSG CN WG 1**

Title: **CRs to Rel-5 on Work Item IMS-CCR towards 24.229,- pack 7**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **5** CRs, **Rel-5** Work Item **"IMS-CCR"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #18 for approval.

Spec	CR #	Rev	CAT	Rel	Tdoc Title	Meeting	TDoc #	C_Version
24.229	279	1	F	Rel-5	Meaning of refresh request	N1-27	N1-022444	5.2.0
24.229	280		F	Rel-5	Removal of Caller Preferences dependency	N1-27	N1-022362	5.2.0
24.229	281	1	F	Rel-5	P-Access-Network-Info clarifications	N1-27	N1-022445	5.2.0
24.229	282		F	Rel-5	Clarification on use of the From header by the UE	N1-27	N1-022370	5.2.0
24.229	287	1	F	Rel-5	SA related procedures	N1-27	N1-022459	5.2.0

3GPP TSG-CN1 Meeting #27 ***Tdoc N1-022444***
Bangkok, Thailand, 11 – 15 November 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **279** ⌘ **rev** **1** ⌘ Current version: **5.2.0** ⌘

*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:	⌘	Meaning of refresh request
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	13/11/2002
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 term "refresh request" is not defined. Its definition is not clear
Summary of change:	⌘	The term "refresh request" is systematically replaced by "target refer request", which in turn is defined in RFC 3261.
Consequences if not approved:	⌘	Missleading implementation when the terminology is not correct

Clauses affected:	⌘	3.1, 5.2.6.2, 5.2.6.3, 5.2.6.4, 5.4.3.1, 5.4.3.2, 5.4.3.3

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.

First proposed change

3 Definitions and abbreviations

3.1 Definitions

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

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

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

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

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

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

Filter criteria
Initial filter criteria
Initial Request

Standalone Transacation
Subsequent Request

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

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

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

User Equipment (UE)

Next proposed change

5.2.6.2 Determination of mobile-originated or mobile-terminated case

Upon receipt of an initial request or a target refresh request or a stand-alone transaction, the P-CSCF shall:

- perform the procedures for the mobile-terminating case as described in subclause 5.2.6.4 if the request makes use of the information for mobile-terminating calls, which was added to the Path header entry of the P-CSCF during registration (see subclause 5.2.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter;
- perform the procedures for the mobile-originating case as described in subclause 5.2.6.3 if this information is not used by the request.

Next proposed change

5.2.6.3 Requests initiated by the UE

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains as P-Asserted-Identity header that matches one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains as P-Asserted-Identity header that does not match one of the registered public user identities, or does not contain a P-Asserted-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity.

NOTE: The contents of the From header do not form any part of this decision process.

When the P-CSCF receives from the UE an initial request for a dialog, and a P-Service-Route header list exists for the initiator of the request, the P-CSCF shall:

1) remove any Route header from the request;
2) select the list of Route headers that was created during the registration or reregistration of the respective public user identity utilizing the P-Service-Route mechanism;
3) pre-load the list of Route headers to the request;
4) create a Record-Route header containing its own SIP URL;
5) insert a P-Asserted-Identity header with a value representing the initiator of the request;
6) create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and
7) forward the request based on the topmost Route header.

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

1) store the values received in the P-Charging-Function-Addresses header;
2) remove the list of Record-Route headers from the received response;
3) create a new list of stored Route headers, with the newly received list of Record-Route headers. The Contact header received in the response shall not be appended to the bottom of the stored list of Route headers;
4) store the dialog ID and associate it with the private user identity and public user identity involved in the session;
5) save the Contact header received in the response in order to release the dialog if needed; and
6) forward the response to the UE.

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

1) remove any list of Record-Route headers, even though not allowed, from the received response; and
2) forward the response to the UE.

When the P-CSCF receives from the UE a target refresh request for a dialog, the P-CSCF shall:

1) verify if the request relates to a dialog in which the originator of the request is involved:
   a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The P-CSCF will not forward the request. No other actions are required;

b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;

2) remove any Route header from the request;

3) select the list of Route headers that was created during the exchange of the initial request and its associated response;

4) pre-load the list of Route headers to the request;

5) create a Record-Route header containing its own SIP URL; and

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

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

1) remove the list of Record-Route headers from the received response;

2) overwrite any existing list of stored Route headers, or create a new list of stored Route headers, with the newly received list of Record-Route headers. The Contact header received in the response shall not be appended to the bottom of the stored list of Route headers;

3) save the Contact header received in the response in order to release the dialog if needed; and4) forward the response to the UE.

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

1) remove any list of Record-Route headers, even though not allowed, from the received response; and

2) forward the response to the UE.

When the P-CSCF receives from the UE the request for a standalone transaction, and a P-Service-Route header list exists for the initiator of the request, the P-CSCF shall:

1) remove any Route header from the request;

2) select the list of Route headers that was created during the registration or reregistration of the respective public user identity utilizing the P-Service-Route mechanism;

3) pre-load the list of Route headers to the request;

4) insert a P-Asserted-Identity header with a value representing the initiator of the request;

5) create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and

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

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) store the values received in the P-Charging-Function-Addresses header; and

2) remove any list of Record-Route headers, even though not allowed, from the received response and forward it to the UE.

When the P-CSCF receives from the UE subsequent requests other than a ~~refreshing~~ target refresh request, the P-CSCF shall:

1) verify if the request relates to a dialog in which the originator of the request is involved:

a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The P-CSCF will not forward the request. No other actions are required;

b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;

2) select the list of Route headers that was created during the exchange of the initial request and associated response for this call;

3) pre-load the list of Route headers to the request; and

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

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) remove any list of Record-Route headers, valid or not, from the received response; and

2) forward the response to the UE.

When the P-CSCF receives from the UE an initial request for a dialog, a target refresh request for a dialog, or the request of a standalone transaction, and a P-Service-Route header list does not exist for the initiator of the request, the P-CSCF shall:

1) send a 403 (Forbidden) response back to the UE containing a warning header.

Editor's Note: how to find out whether the user has a valid registration in the P-CSCF is FFS.

Editor's Note: The correct value for the warning code is yet to be assigned by IANA.

When the P-CSCF receives from the UE the request for an unknown method, and a P-Service-Route header list exists for the initiator of the request, the P-CSCF shall:

1) select the list of Route headers that was created during the registration or reregistration of the respective public user identity utilizing the P-Service-Route mechanism;

2) pre-load the list of Route headers to the request,

3) insert an P-Asserted-Identity header with a value representing the initiator of the request; and

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

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) remove any list of Record-Route headers, even though invalid, from the received response; and

2) forward the response to the UE.

Next proposed change

5.2.6.4 Requests terminated by the UE

When the P-CSCF receives a response to an initial request for a dialog or a response to a request for a standalone transaction, the P-CSCF shall identify responder by a public user identity that relates to the Request-URI used in the request.

NOTE: The contents of the To header do not form any part of this decision process.

When the P-CSCF receives, destined for the UE, an initial request for a dialog, or a target refresh request for a dialog, prior to forwarding the request, the P-CSCF shall:

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

2) remove the list of Record-Route headers, and shall convert it into a list of Route headers. The Contact header shall not be appended to the bottom of the list of Route headers. The P-CSCF shall save this list of Route headers and append this list to all UE originated requests for this dialog;

3) save the Contact header received in the response in order to release the dialog if needed;

4) add itself on the top of the removed list of Record-Route headers and save the list. The list will be appended to UE originated response to the SUBSCRIBE request;

5) remove and store the list of received Via headers from the received request and shall place its own address in the Via header with locally unique token to identify the saved values as a branch parameter. The P-CSCF shall append the list of Via headers to the UE originated response for this request;

6) store the values received in the P-Charging-Function-Addresses header; and

7) remove and store the icid parameter received in the P-Charging-Vector header.

When the P-CSCF receives a 1xx or 2xx response to the above request, the P-CSCF shall:

1) insert an P-Asserted-Identity header with a value representing the responder to the request;

2) append the saved list of Record-Route headers to the response;

3) append the saved list of Via headers to the response; and

4) store the dialog ID and associate it with the private user identity and public user identity involved in the session.

When the P-CSCF receives any other response to the above request, the P-CSCF shall:

1) append the saved list of Via headers to the response.

When the P-CSCF receives, destined for the UE, a request for a stand-alone transaction, prior to forwarding the request, the P-CSCF shall:

1) insert an P-Asserted-Identity header with a value representing the responder to the request;

2) remove and store the list of received Via headers from the received request and shall place its own address in the Via header with locally unique token to identify the saved values as a branch parameter. The P-CSCF shall append this list of Via headers to the UE originated response for this transaction;

3) store the values received in the P-Charging-Function-Addresses header; and

4) remove and store the icid parameter received in the P-Charging-Vector header.

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) append the saved list of Via headers to the response.

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a target refresh request, prior to forwarding the request, the P-CSCF shall:

1) remove and store the list of received Via headers from the received request and shall place its own address in the Via header with locally unique token to identify the saved values as a branch parameter. The P-CSCF shall append this list of Via headers to the UE originated response for this transaction; and

2) remove and store the icid parameter from P-Charging-Vector header.

When the P-CSCF receives any response to the above request, the P-CSCF shall:

1) append the saved list of Via headers to the response.

Next proposed change

5.4.3.1 Determination of mobile-originated or mobile-terminated case

Upon receipt of an initial request or a target refresh request or a stand-alone transaction, the S-CSCF shall:

- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the request makes use of the information for mobile-originating calls, which was added to the Path header entry of the S-CSCF during registration (see subclause 5.4.1.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter; or,

- perform the procedures for the mobile-terminating case as described in subclause 5.4.3.3 if this information is not used by the request.

Next proposed change

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 an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request;

- check whether the initial request matches the initial filter criteria based on a public user identity in the P-Asserted-Identity header, 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 populated as specified in the subclause 5.4.3.4;

- 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 orig-ioi parameter into the P-Charging-Vector header if the next hop is an AS, I-CSCF or outside of the current network. The orig-ioi parameter shall be set to a value that identifies the sending network. The term-ioi 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 target 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 target 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 a target 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;

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

- route the request based on the topmost Route header.

Next proposed change

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 an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request;

3) check whether the initial request matches the initial filter criteria based on the public user identity in the Request-URI, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

   insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL populated as specified in the subclause 5.4.3.4;

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 orig-ioi parameter received in the P-Charging-Vector header, if present. The orig-ioi parameter identifies the sending network of the request message. The orig-ioi 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 target 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 target refresh request in order to release the dialog when needed; and

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

When the S-CSCF receives a response to the target 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 target 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).

3GPP TSG-CN1 Meeting #27 ***Tdoc N1-022362***
Bangkok, Thailand, 11 – 15 November 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **280** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

*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:	⌘	Removal of Caller Preferences dependency
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	29/10/2002
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:	⌘	Latest version of the MESSAGE draft does not depend on Caller Preferences
Summary of change:	⌘	The dependency on Caller Preferences is removed The reference to the MESSAGE method draft is updated
Consequences if not approved:	⌘	Innecessary implementation of an Internet Draft The Internet Draft path to become RFC is not clear… It may take too long to get an RFC number for the Release 5 time frame.

Clauses affected:	⌘	2, 5.1.1.2

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.

First proposed change

2 References

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

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

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.002: "Network architecture".

[3] 3GPP TS 23.003: "Numbering, addressing and identification".

[4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[5] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".

[6] 3GPP TS 23.221: "Architectural requirements".

[7] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".

[8] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".

[9] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".

[10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".

[10A] 3GPP TS 27.060: "Mobile Station (MS) supporting Packet Switched Services".

[11] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN)".

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

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

[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 (June 1999): "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-ietf-sip-refer-05 (June 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-03 (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-06 (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-10 (May 2002): "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-dhcpv6-26 (June 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-03.txt (July 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-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] Void.

[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.

[50] draft-ietf-sip-message-~~06~~07.txt (~~July~~ September 2002): "Session Initiation Protocol Extension for Instant Messaging"

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

[51] void~~draft-ietf-sip-callerprefs-06.txt (July 2002): "Session Initiation Protocol (SIP) Caller Preferences and Callee Capabilities"~~

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

Next proposed change

5.1.1.2 Initial registration

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

~~As the UE supports the SIP MESSAGE method, at registration time the UE shall add the ";methods" tag to the Contact header, with an indication of support of the MESSAGE method, according to the procedures described in the SIP MESSAGE method draft-ietf-sip-message-06 [50], and in the Caller Preferences draft-ietf-sip-callerprefs-06.txt [51].~~

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;

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

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.

3GPP TSG-CN1 Meeting #27 ***Tdoc N1-022445***
Bangkok, Thailand, 11 – 15 November 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **281** ⌘ **rev** **1** ⌘ Current version: **5.2.0** ⌘

*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:	⌘	P-Access-Network-Info clarifications
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	13/11/2002
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:	⌘	According to the current procedures, the S-CSCF will remove the P-Access-Network-Info header prior to the request reaching an Application Server. This will prevent ASes to provide services based on the contents of the header.
Summary of change:	⌘	Clarified that the S-CSCF removes the P-Access-Network-Info when it forwards the SIP request or response to the destination network or to an application server that is located outside the trust domain. Clarified that the P-Access-Network-Info is used by the Application Server. Removed the unconcrete required actions to act upon accordingly.
Consequences if not approved:	⌘	Application Servers will not be able to provide services based on the P-Access-Network-Info header. Not clear requirements in the S-CSCF as with respect the P-Access-Network-Info header.

Clauses affected:	⌘	4.4, 5.4, 5.7, 7.2.3

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.

First proposed change

4.4 Trust domain ~~for asserted identity~~

RFC 3325 [34] provides for the existence and trust of an asserted identity within a trust domain. For the IM CN subsystem, this trust domain consists of the P-CSCF, the I-CSCF, the S-CSCF, the BGCF. the MGCF, the MRFC, and all ASs that are not provided by third-party service providers. ASs provided by third-party service providers are outside the trust domain.

For the purpose of the P-Access-Network-Info header, a trust domain also applies. This trust domain is identical to that of the P-Asserted-Identity.

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

Next proposed change

5.4 Procedures at the S-CSCF

5.4.1 Registration and authentication

5.4.1.1 Introduction

The S-CSCF shall act as the SIP registrar for all UAs of the IM CN subsystem with public user identities.

The S-CSCF shall support the use of the Path and P-Service-Route header. The S-CSCF must also support the Require and Supported headers. The Path header is only applicable to the REGISTER request and its 200 (OK) response. The P-Service-Route header is only applicable to the 200 (OK) response of REGISTER.

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

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

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

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Unprotected REGISTER

NOTE 1: Any REGISTER request sent unprotected by the UE is considered to be an initial registration. A 200 (OK) final response to such a request will only be sent back after the S-CSCF receives a correct RES in an integrity protected sent REGISTER.

Upon receipt of a REGISTER request with the integrity-protection parameter set to 'no', the S-CSCF shall:

1) identify the user by the public user identity as received in the To header and the private user identity as received in the username field in the Authorization header of the REGISTER request;

2) check if the P-Visited-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;

3) check the value of the Expires header. The S-CSCF shall only proceed with the following procedures if the Expires header is set to a value greater than zero; if the Expires header is set to a value zero, then S-CSCF shall proceed according to subclause 5.4.1.4;

4) check how many authentications are ongoing for this user. The S-CSCF may – based on local policy – reject the request by sending a 403 (Forbidden) response, if there are a number of ongoing authentications. If the S-CSCF decides to challenge the user, then proceed as follows;

5) select an authentication vector for the user. If no authentication vector for this user is available, after the S-CSCF has performed the Cx Multimedia Authentication procedure with the HSS, as described in 3GPP TS 29.229 [15], the S-CSCF shall select an authentication vector as described in 3GPP TS 33.203 [19].

   Prior to performing Cx Multimedia Authentication procedure with the HSS, the S-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];

NOTE 2: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URL to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

6) store the icid parameter received in the P-Charging-Vector header;

~~7) remove the P-Access-Network-Info header and may act upon the contents accordingly;~~

7~~8~~) challenge the user by generating a 401 (Unauthorized) response for the received REGISTER request, including a WWW-Authenticate header which transports:

- the home network identification in the realm field;
- the RAND and AUTN parameters and optional server specific data for the UE in the nonce field;
- the security mechanism, which is AKAv1-MD5, in the algorithm field;
- the IK (Integrity Key) parameter for the P-CSCF in the ik field (see subclause 7.2.3);
- optionally the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2.3);

8~~9~~) send the so generated 401 (Unauthorized) response towards the UE; and,

9~~10~~) start timer reg-await-auth which guards the receipt of the next REGISTER request.

5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the integrity-protection parameter set to 'yes', the S-CSCF shall:

In the case that there is no authentication currently ongoing for this user (i.e. no timer reg-await-auth is running):

1) identify the user by the public user identity as received in the To header and the private user identity as received in the From header of the REGISTER request;

2) check if the user needs to be reauthenticated.

   The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for registration requests received without integrity protection by the P-CSCF. The information that a REGISTER request was received integrity protected at the P-CSCF may be used as part of the decision to challenge the user.

   If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph; and

3) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall proceed with the procedures as described for the second REGISTER in subclause 5.4.1.2, beginning with step 7); ~~and~~

~~4) remove the P-Access-Network-Info header and may act upon the contents accordingly.~~

In the case that a timer reg-await-auth is running for this user the S-CSCF shall:

1) identify the user by the public user identity as received in the To header and the private user identity as received in the username field in the Authorization header of the REGISTER request;

2) check if the Call-ID of the request matches with the Call-ID of the 401 (Unauthorized) response which carried the last challenge. The S-CSCF shall only proceed further if the Call-IDs match.

3) stop timer reg-await-auth;

4) check whether an Authorization header is included, containing:

   - the private user identity of the user in the username field;
   - the algorithm which is AKAv1-MD5 in the algorithm field; and

- the RES parameter needed for the authentication procedure in the response field.

The S-CSCF shall only proceed with the following steps in this paragraph if the RES parameter was included;

5) check whether the received RES parameter and the XRES parameter match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if RES and XRES are matching;

6) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], store the following information in the local data:

- the list of public user identities associated to the user, including the own public user identity under registration and the implicitly registered due to the received REGISTER request. Each public user identity is identified as either barred or non-barred; and,

- the user profile(s) of the user including initial Filter Criteria;

NOTE 1: There might be more than one set of initial Filter Criteria received because some implicitly registered public user identities that are part of the same user's subscription may belong to different service profiles.

7) bind to each non-barred registered public user identity all registered contact information and store the related method tag values from the Contact header for future use;

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

NOTE 3: The barred public user identities are not bound to the contact information.

8) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

9) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;

10) store the icid parameter received in the P-Charging-Vector header;

~~11) remove the P-Access-Network-Info header and may act upon the contents accordingly;~~

~~12~~11) create a 200 (OK) response for the REGISTER request, including:

- an expiration time in the Expires header, using one value provided within the S-CSCF, and,

- the list of received Path headers;

- a P-Associated-URI header containing the list of public user identities that the user is authorized to use. Such a collection of public user identities may or may not be implicitly registered by the network. Using information supplied by the HSS, the P-Associated-URI header will indicate the default public user identity to be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header;

Editor's note: The mechanism for indicating this default public user identity is yet to be agreed.

- a P-Service-Route header containing:

  - the SIP URL identifying the S-CSCF; and,

  - an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) shall be treated as for the mobile-originating case. This indication may e.g. be in a URI parameter, a character string in the user part or be a port number;

  - if network topology hiding is required a SIP URL identifying an I-CSCF(THIG) as the topmost entry;

~~13~~12) send the so created 200 (OK) response to the UE;

~~14~~13) 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; and,

NOTE 5: If this registration is a reregistration, the Filter Criteria already exists in the local data.

~~15~~14) handle the user as registered for the duration indicated in the Expires header.

5.4.1.2.3 Abnormal cases

The S-CSCF need not challenge an unprotected REGISTER request for a private user identity that already has a registration in process, but instead return a 500 (Server Internal Error) response. The response shall contain a Retry-After header with a value indicating a time the UE shall wait before resending the request.

In the case that the authentication response (RES) from the UE does not match with XRES and the request was correctly integrity protected (it is indicated by the P-CSCF), or the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), and the authentication response was triggered by an initial registration or a UE initiated reauthentication, the S-CSCF shall either:

- start a network initiated re-authentication procedure as defined in subclause 5.4.1.6; or

- send a further challenge 401 (Unauthorized) to the UE.

In the case that the authentication response (RES) from the UE does not match with XRES and the request was correctly integrity protected (it is indicated by the P-CSCF), or the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), and the authentication response was triggered by a network initiated reauthentication the S-CSCF shall either:

- attempt a further authentication challenge; or

- deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the REGISTER request from the UE containing an authentication response indicates that the authentication challenge was invalid and with no RES or AUTS parameter, the S-CSCF shall:

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

In the case that the REGISTER request from the UE containing an authentication response indicates that the authentication challenge was invalid but contains the AUTS parameter, the S-CSCF will fetch new authentication vectors from the HSS, including AUTS and RAND in the request to indicate a resynchronisation. On receipt of these vectors from the HSS, the S-CSCF shall:

- send a 401 Unauthorized to initiate a further authentication attempt, using these new vectors.

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

- reject the REGISTER request with a 423 (Interval Too Brief) response, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

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

5.4.1.3 Authentication and reauthentication

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

5.4.1.4 User-initiated deregistration

When 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 Authorization 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; and

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

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 Authorization 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.

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 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.

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 reg 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 "reg" 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 the state parameter set to "terminated" and the event parameter set to "deactivated".

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 with which it can authenticate the subscriber, the S-CSCF may use other means to request the UE to re-authenticate, e.g. by sending a REFER method in order to request a registration.

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 all public user identities associated with the private user identity, as described in subclause 5.4.1.5, and terminate the ongoing sessions of that user.

5.4.1.7 Notification of Application Servers about registration status

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

a) the Request-URI shall contain the AS's SIP URL;

b) the From header shall contain the S-CSCF's SIP URL;

c) the To header shall contain either the public user identity as contained in the REGISTER request received from the UE or one of the implicitly registered public user identities, as configured by the operator;

d) the Contact header shall contain the S-CSCF's SIP URL;

e) for initial registration and user-initiated reregistration (subclause 5.4.1.2), the Expires header shall contain the same value that the S-CSCF returned in the 200 (OK) response for the REGISTER request received form the UE;

f) for user-initiated deregistration (subclause 5.4.1.4) and network-initiated deregistration (subclause 5.4.1.5), the Expires header shall contain the value zero;

g) for initial registration and user-initiated reregistration (subclause 5.4.1.2), a message body shall be included in the REGISTER request if there is Filter Criteria indicating the need to include HSS provided data for the REGISTER event (e.g. HSS may provide AS specific data to be included in the third-party REGISTER, such as IMSI to be delivered to IM SSF). If there is a service information XML element provided in the HSS Filter Criteria for an AS (see 3GPP TS 29.228 [14]), then it shall be included in the message body of the REGISTER request within the <service-info> XML element as described in subclause 7.6. For the messages including the 3GPP IMS XML body, set the value of the Content-Type header to include the MIME type specified in subclause 7.6;

h) for initial registration, the P-Charging-Vector header shall contain the same icid parameter that the S-CSCF received in the original REGISTER request from the UE;

i) for initial registration, a P-Charging-Function-Addresses header (see subclause 7.2.5) shall be populated with values received from the HSS if the message is forwarded within the S-CSCF home network.

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 reg 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 reg 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 "reg" 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 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;
- set state parameter in the <contact> elements to "active" for all public user identities which are currently registered;
- set state parameter in the <contact> element to "terminated" for all public user identities which are currently deregistered; and
- indicate those public user identities which will be automatically reregistered 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.

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>
```

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

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

5.4.3.1 Determination of mobile-originated or mobile-terminated case

Upon receipt of an initial request or a refresh request or a stand-alone transaction, the S-CSCF shall:

- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the request makes use of the information for mobile-originating calls, which was added to the Path header entry of the S-CSCF during registration (see subclause 5.4.1.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter; or,
- perform the procedures for the mobile-terminating case as described in subclause 5.4.3.3 if this information is not used by the request.

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 an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request;

- check whether the initial request matches the initial filter criteria based on a public user identity in the P-Asserted-Identity header, 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 populated as specified in the subclause 5.4.3.4; and

  - if the AS is located outside the trust domain then the S-CSCF shall retain the P-Access-Network-Info header field and its values in the request; if the AS is located within the trust domain, then the S-CSCF shall remove the P-Access-Network-Info header field and its values in the request.

- 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 orig-ioi parameter into the P-Charging-Vector header if the next hop is an AS, I-CSCF or outside of the current network. The orig-ioi parameter shall be set to a value that identifies the sending network. The term-ioi 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;

- in case the request is forwarded to the destination network network or to an AS located outside the trust domain, 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;

- in case the request is forwarded to the destination network or to an AS located outside the trust domain, 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;~~

- in case the request is forwarded to the destination network or to an AS located outside the trust domain, 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 an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request;

3) check whether the initial request matches the initial filter criteria based on the public user identity in the Request-URI, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

   insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL populated as specified in the subclause 5.4.3.4;

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 orig-ioi parameter received in the P-Charging-Vector header, if present. The orig-ioi parameter identifies the sending network of the request message. The orig-ioi 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. In case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header.

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) 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. In case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header.

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

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).

5.4.3.4 Original dialog identifier

The original dialog identifier is an implementation specific token that the S-CSCF encodes into the own S-CSCF URL in a Route header, prior to forwarding the request to an application server. This is possible because the S-CSCF is the only entity that creates and consumes the value.

The token identifies the original dialog of the request, so in case an application server acting as a B2BUA changes the dialog, the S-CSCF is able to identify the original dialog when the request returns to the S-CSCF. The token can be encoded in different ways, such as e.g., a character string in the user-part of the S-CSCF URL, a parameter in the S-CSCF URL or port number in the S-CSCF URL.

The S-CSCF shall ensure that the value chosen is unique so that the S-CSCF may recognize the value when received in a subsequent message and make the proper association between related dialogs that pass through an Application Server.

5.4.3.5 Void

5.4.4 Call initiation

5.4.4.1 Initial INVITE

Void.

5.4.4.2 Subsequent requests

5.4.4.2.1 Mobile-originating case

When the S-CSCF receives the 183 response, the S-CSCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present. The term-ioi parameter identifies the sending network of the response message. The term-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS.

When the S-CSCF receives the 183 response, the S-CSCF shall 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.

When the S-CSCF receives the UPDATE request, the S-CSCF shall store the 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

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.

When the S-CSCF receives any request or response related to a mobile-originated dialog or standalone transaction, the S-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message within the S-CSCF home network, including towards AS.

5.4.4.2.2 Mobile-terminating case

When the S-CSCF sends the 183 response, the S-CSCF shall insert an term-ioi parameter in the P-Charging-Vector header of the outgoing response if the response is sent to another network, an AS or an I-CSCF. The term-ioi parameter shall be set to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi.

When the S-CSCF receives the 183 response, the S-CSCF shall 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.

When the S-CSCF receives 180 (Ringing) or 200 (OK) (to INVITE) responses, the S-CSCF shall store the 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 an AS. However, the gprs-charging-info parameter shall not be included in the P-Charging-Vector header when the response is forwarded outside the home network of the S-CSCF.

When the S-CSCF receives any request or response related to a mobile-originated dialog or standalone transaction, the S-CSCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message within the S-CSCF home network, including towards AS.

5.4.5 Call release

5.4.5.1 S-CSCF-initiated session release

5.4.5.1.1 Cancellation of a session currently being established

Upon receipt of an network internal indication to release a session which is currently being established, the S-CSCF shall cancel the related dialogs by sending the CANCEL request according to the procedures described in RFC 3261 [26].

5.4.5.1.2 Release of an existing session

Upon receipt of a network internal indication to release an existing multimedia session, the S-CSCF shall:

1) generate a first BYE request for the called user based on the information saved for the related dialog, including:
   - a Request-URI, set to the stored Contact header provided by the called user;
   - a To header, set to the To header value as received in the 200 OK response for the initial INVITE request;
   - a From header, set to the From header value as received in the initial INVITE request;
   - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
   - a CSeq header, set to the CSeq value that was stored for the direction from the calling to the called user, incremented by one;
   - a Route header, set to the routeing information towards the called user as stored for the dialog;
   - further headers, based on local policy or the requested session release reason.
2) generate a second BYE request for the calling user based on the information saved for the related dialog, including:
   - a Request-URI, set to the stored Contact header provided by the calling user;

- a To header, set to the From header value as received in the initial INVITE request;
- a From header, set to the To header value as received in the 200 OK response for the initial INVITE request;
- a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
- a CSeq header, set to the CSeq value that was stored for the direction from the called to the calling user, incremented by one – if no CSeq value was stored for that session it shall generate and apply a random number within the valid range for CSeqs;
- a Route header, set to the routeing information towards the calling user as stored for the dialog;
- further headers, based on local policy or the requested session release reason.

3) if the S-CSCF serves the calling user, treat the first BYE request as if received directly from the calling user, i.e. send it to internal service control and based on the outcome further on towards the called user;
4) if the S-CSCF serves the calling user, send the second BYE request directly to the calling user.
5) if the S-CSCF serves the called user, send the first BYE request directly to the called user;
6) if the S-CSCF serves the called user, treat the second BYE request as if received directly from the called user, i.e. shall send it to internal service control and based on the outcome further on towards to the called user.

Upon receipt of the 2xx responses for both BYE requests, the S-CSCF shall release all information related to the dialog and the related multimedia session.

5.4.5.1.3 Abnormal cases

Upon receipt of a request on a dialog for which the S-CSCF initiated session release, the S-CSCF shall terminate the received request and answer it with a 481 (Call/Transaction Does Not Exist) response.

5.4.5.2 Session release initiated by any other entity

Upon receipt of a 2xx response for a BYE request matching an existing dialog, the S-CSCF shall delete all the stored information related to the dialog.

5.4.6 Call-related requests

5.4.6.1 ReINVITE

5.4.6.1.1 Determination of served user

Void.

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, if the request is to be forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header.~~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)~~any SIP response to an INVITE, if the response is to be forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. ~~the S-CSCF shall also remove the P-Access-Network-Info header and may act upon its contents accordingly~~.

5.4.7 MESSAGE support

A S-CSCF may be capable of sending and/or receiving the MESSAGE method to conduct session-unrelated or session related interactions. To do so, a S-CSCF may initiate or terminate the MESSAGE method per draft-ietf-sip-message-06.txt [50]. The S-CSCF should support, as a minimum, a body of type “text/plain” per draft-ietf-sip-message-06.txt [50].

The size of the payload in a SIP MESSAGE may vary significantly. When the size of the whole SIP MESSAGE request exceeds 1300 bytes, the S-CSCF shall use TCP transport protocol for sending the MESSAGE request.

Next proposed change

5.7 Procedures at the Application Server (AS)

NOTE: This subclause defines only the requirements on the application server that relate to SIP. Other requirements are defined in 3GPP TS 23.218 [5].

5.7.1 Common Application Server (AS) Procedures

5.7.1.1 Notification about registration status

The AS may support the REGISTER method in order to discover the registration status of the user. If a REGISTER request arrives containing information about the user's registration status and the AS supports the REGISTER method, the AS shall store the Expires parameter from the request and generate a 200 (OK) response or an appropriate failure response. For the success case, the 200 (OK) response shall contain Expires value equal to the value received in the REGISTER request. The AS shall store the values received in P-Charging-Function-Addresses header.Also, the AS shall store the values of the icid parameter in the P-Charging-Vector header from the REGISTER request.

5.7.1.2 Extracting charging correlation information

When an AS receives an initial request for a dialog or a request for a standalone transaction, the AS shall store the values received in the P-Charging-Vector header, e.g. icid parameter, and retain the P-Charging-Vector header in the message. The AS shall store the values received in the P-Charging-Function-Addresses header and retain the P-Charging-Function-Addresses header in the message.

When an AS sends any request or response related to a dialog or standalone transaction, the AS may insert previously saved values into the P-Charging-Vector and P-Charging-Function-Addresses headers before sending the message.

5.7.1.4 Access-Network-Info

The AS may receive in any request or response information about the served user access network. This information is contained in the P-Access-Network-Info header. The AS can use the header to provide an appropriate service to the user.

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

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

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

An Application Server acting as redirect server shall propagate any received 3GPP message body in the redirected message.

5.7.3 Application Server (AS) acting as originating UA

When acting as an originating UA the AS shall behave as defined for a UE in subclause 5.1.3, with the exceptions noted in this subclause.

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

When an AS acting as an originating UA generates an initial request for a dialog or a request for a standalone transaction, the AS shall create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header.

Furthermore the AS shall insert a Route header pointing to the S-CSCF.

5.7.4 Application Server (AS) acting as a SIP proxy

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

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

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

An Application Server acting as a SIP proxy shall propagate any received 3GPP message body in the forwarded message.

5.7.5 Application Server (AS) performing 3rd party call control

5.7.5.1 General

The AS performing 3rd party call control acts as a B2BUA. There are two kinds of 3rd party call control:

- Routeing B2BUA: an AS receives a request from S-CSCF, terminates it and generates a new request, which is based on the received request.
- Initiating B2BUA: an AS initiates two requests, which are logically connected together at the AS.

The B2BUA AS will internally map the message headers between the two dialogs that it manages. It is responsible for correlating the dialog identifiers and will decide when to simply translate a message from one dialog to the other, or when to perform other functions. These decisions are specific to each AS and are outside the scope of the present document.

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

5.7.5.2 Call initiation

5.7.5.2.1 Initial INVITE

When the AS acting as a Routeing B2BUA receives an initial INVITE request from the S-CSCF, the AS shall:

- remove its own SIP URL from the topmost Route header of the received INVITE request;
- perform the Application Server specific functions. See 3GPP TS 23.218 [5];
- if successful, generate and send a new INVITE request to the S-CSCF to establish a new dialog;
- copy the remaining Route header(s) unchanged from the received INVITE request to the new INVITE request;
- route the new INVITE request based on the topmost Route header.

NOTE: The topmost Route header of the received INVITE request will contain the AS's SIP URI. The following Route header will contain the SIP URI of the S-CSCF.

When the AS acting as an Initiating B2BUA the AS shall apply the procedures described in subclause 5.7.3 for both requests. The AS shall either set the icid parameter in the P-Charging-Vector header to be the same as received or different.

5.7.5.2.2 Subsequent requests

Void.

5.7.5.3 Call release

5.7.5.4 Call-related requests

An Application Server may initiate a call release. See 3GPP TS 23.218 [5] for possible reasons. The BYE request shall be sent simultaneously for both dialogs managed by the B2BUA.

5.7.5.5 Further initial requests

Void.

5.7.6 MESSAGE support

An application server (AS) may be capable of sending and/or receiving the MESSAGE method to conduct session-unrelated or session related interactions. To do so, the AS may initiate or terminate MESSAGE requests per draft-ietf-sip-message-06.txt [50]. The AS should support, as a minimum, a body of type “text/plain” per draft-ietf-sip-message-06.txt [50].

The size of the payload in a SIP MESSAGE may vary significantly. When the size of the whole SIP MESSAGE request exceeds 1300 bytes, the AS shall use TCP transport protocol for sending the MESSAGE request.

Next proposed change

7.2.3 P-Access-Network-Info header

7.2.3.1 Introduction

The P-Access-Network-Info header is the mechanism whereby the UE provides the ~~S-CSCF~~Application Server with information relating to the access network it is using. This may include the cell ID.

The UE shall insert the P-Access-Network-Info header into all requests or responses it originates.

~~The S-CSCF~~ When forwarding a request or response to an AS that is located within the trust domain, the S-CSCF will retain the P-Access-Network-Info header; otherwise, the S-CSCF ~~shall~~ will remove the P-Access-Network-Info header from any message where it is present~~, before it forwards the message~~. ~~The S-CSCS shall act accordingly upon the information received in the P-Access-Network-Info header.~~

When the S-CSCF sends a 3rd party REGISTER request to an AS that is located within the trust domain, the S-CSCF will include the P-Access-Network-Info header received in the REGISTER request from the UE. If the AS is not located within the trust domain, then the S-CSCF will not include any P-Access-Network-Info header.

7.2.3.2 Syntax

The syntax of the P-Access-Network-Info header is described in draft-mills-sip-access-network-info-02.txt [47].

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 "~~CGI-3GPP~~cgi-3gpp" parameter. This value shall be the Cell Global Identity obtained from lower layers of the UE.

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

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

If the *access type* field is equal to "3GPP-UTRAN-FDD", "3GPP-UTRAN-TDD" or "3GPP-CDMA2000" the *access info* field shall contain a value for "~~UTRAN-CELL_ID-3GPP~~utran-cell-id-3gpp" parameter. This value shall be made up of a concatenation of the MCC, MNC, LAC (as described in 3GPP TS 23.003) 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).

First proposed change

5.1.2A Generic procedures applicable to all methods

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 t~~The contents of the From header should not be relied upon to be ~~are~~ modified by the network based on any privacy specified by the user either within the UE indication of privacy or by network subscription or network policy. Therefore the user ~~could require to~~should include the value "Anonymous" ~~even on requests where~~whenever privacy is ~~not explicitly requested~~required. As the user may well have privacy requirements, terminal manufacturers should not automatically derive and include values in this header from the public user identity or other values stored in the USIM. Where the user has not expressed a preference in the configuration of the terminal implementation, the implementation should assume that privacy is required. Users that require to identify themselves, and are making calls to SIP destinations beyond the IM CN subsystem, where the destination does not implement RFC 3325 [34], will need to include a value in the From header other than Anonymous.

The UE can indicate privacy of the P-Asserted-Identity 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).

Next proposed change

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 an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request;

3) check whether the initial request matches the initial filter criteria based on the public user identity in the Request-URI, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

   insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL populated as specified in the subclause 5.4.3.4;

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 orig-ioi parameter received in the P-Charging-Vector header, if present. The orig-ioi parameter identifies the sending network of the request message. The orig-ioi 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) 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).

3GPP TSG-CN1#26 ***Tdoc ⌘N1-022382***
Bangkok, Thailand, 11-15 November 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **287** ⌘ **rev** **1** ⌘ Current version: **5.2.0** ⌘

*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⌘ [X] ME [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	SA related procedures
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	05/11/2002
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:	⌘	~~In case of re-authentication, it is not specified how long to use the old derived keys and when to start using the new keys.~~Rewording was needed in some places, in comparison to the originally submitted CR. Additionally a change to one of the paragraphs has been removed from some collided CRs and implemented instead in this CR.
Summary of change:	⌘	Rewording.~~Clarification text has been added to both the UE and P-CSCF part.~~
Consequences if not approved:	⌘	The text perhaps will be confusing.~~A reauthentication may result in not using the same set of keys in the UE and P-CSCF side, which means failure in communication.~~

Clauses affected:	⌘	5.1.1.4; 5.1.1.5.1; 5.1.1.5.3; 5.1.1.6; 5.2.2

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.

5.1.1.4 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 shall be integrity protected using IK, see 3GPP TS 33.203 [19], received in an earlier registration, if 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; and

e) 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 1: 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.

NOTE 2: 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.

5.1.1.5.1 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; and

- 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~~ derive~~d~~ the keys ~~(~~CK and IK~~) to protect future messages, see 3GPP TS 33.203 [19]~~; ~~and~~

- set up the security association based on the static list it received in the 401 (Unauthorised) and its capabilities sent in the Security-Client header in the REGISTER request. The UE shall set up the security association ~~shall be set up~~ using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using CK and IK as shared keys; 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. 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.

On receiving the 200 (OK) for the integrity protected REGISTER request, the UE shall start using the security association the 200 (OK) was protected with.

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.

5.1.1.5.3 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. The REGISTER request shall be protected with the existing keys (CK and IK) if available, see 3GPP TS 33.203 [19].

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.

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

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) 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 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 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; and

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

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

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]; and

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 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) store the values received in the P-Charging-Function-Addresses header; and

7) update the SIP level lifetime of the security association with the value found in the Expires header.

8) ~~forward~~ protect the response ~~to the UE protected~~ within the same security association to~~in which~~that in which the associated request ~~this response relates to~~ was protected.

9) ~~in case there are multiple security associations set up towards the same UE, the P-CSCF shall not delete any of them until it receives a message from the UE protected with the security association the 200 (OK) as a response to the latest authentication was protected with. When a message protected within this security association is received, the P-CSCF shall~~ delete all earlier security associations and related keys it may have towards the UE, when a message protected within the newly set up security association is received.

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 security association from the IPSec database when their SIP level lifetime expires.