3GPP TSG CN Plenary Meeting #17 **NP-020375**
4th - 6th September 2002. Biarritz, France.

Source: **TSG CN WG 1**

Title: **CRs to Rel-5 on Work Item IMS-CCR towards 24.229,- pack 1**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **6** CRs on **Rel-5 to** Work Item **"IMS-CCR"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #17 for approval.

CR#140r1 has corresponding CRs in 3GPP TS 27.060 and 3GPP TS 29.207.

Spec	CR #	Rev	CAT	Rel	Tdoc Title	Meeting	TDoc #	C_Version
24.229	140	1	F	Rel-5	Support of non-IMS forking.	N1-25	N1-021812	5.1.0
24.229	141	1	F	Rel-5	Adding MESSAGE to 24.229	N1-25	N1-021814	5.1.0
24.229	142		F	Rel-5	Public user identity to use for third party register	N1-25	N1-021563	5.1.0
24.229	143	1	F	Rel-5	Replace P-Original-Dialog-ID header with unique data in Route header	N1-25	N1-021797	5.1.0
24.229	145		F	Rel-5	Synchronize text with latest I-D for P-headers for charging	N1-25	N1-021569	5.1.0
24.229	146	1	F	Rel-5	Service profiles and implicitly registered public user identities	N1-25	N1-021815	5.1.0

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 ~~form~~ from the UE or one of the implicitly registered public user identities, ~~depending on operator~~as configured by the operator~~ation~~;

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.

Start of first changes

4.5 Charging correlation principles for IM CN subsystems

4.5.1 Overview

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

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

1. IMS Charging Identifier (ICID);
2. Access network information:
   a. GPRS Charging Information;
3. Inter Operator Identifier (IOI);
4. Charging function addresses:
   a. Charging Collection Function (CCF);
   b. Event Charging Function (ECF).

The charging correlation information is encoded in the P-Charging-Vector header as defined in subclause 7.2. The P-Charging-Vector header contains the following parameters: icid, access network information and ioi. The parameters are described further in the subclauses that follow. The GGSN provides the access network information to the IM CN subsystem, which is the common information used to correlate GGSN CDRs with IM CN subsystem CDRs.

The offline and online charging function addresses are encoded in the P-Charging-Function-Addresses as defined in subclause 7.2. The P-Charging-Function-Addresses header contains the following parameters: ~~ccf~~ CCF and ~~ecf~~ECF.

4.5.2 IMS charging identifier (ICID)

The IMS Charging Identifier (ICID) is the session level data shared among the IMS network entities including ASs in both the calling and called IMS networks.

The first IMS network entity involved in a dialog (session) or standalone (non-session) message will generate the ICID and include it in the icid parameter of the P-Charging-Vector header in the SIP request. The P-CSCF will generate ICID for mobile originated calls. The I-CSCF will generate ICID for mobile terminated calls if there is no ICID received in the initial request (e.g. the calling party network is another SIP based network). The AS will generate ICID when acting as an originating UA. The MGCF will generate ICID for PSTN/PLMN originated calls. Each entity that processes the SIP request will extract the ICID for possible later use in a charging data records (CDR). The I-CSCF and S-CSCF are also allowed to generate a new ICID for mobile terminated calls received from another network.

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

The icid parameter is included in any requests that include the P-Charging-Vector header. However, the P-Charging-Vector (and ICID) is not passed to the UE. ~~It is also possible for the ICID to be passed to the GGSN and SGSN, but that is outside the scope of this specification.~~

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

4.5.3 Access network information

4.5.3.1 General

The access network information are the media component level data shared among the IMS network entities for one side of the session (either the calling or called side). GPRS charging information (GGSN identifier and GCIDs) is an example of access network information.

4.5.3.2 GPRS charging information

The P-CSCF provides the GPRS charging information to the S-CSCF. The S-CSCF may also pass the information to an Application Server (AS), which may be needed for online pre-pay applications. The GPRS charging information for the originating network is used only within that network, and similarly the GPRS charging information for the terminating network is used only within that network. Thus the GPRS charging information are not shared between the calling and called networks. The GPRS charging information is not passed towards the external ASs from its own network.

The GPRS charging information is populated in the P-Charging-Vector using the gprs-charging-info parameter. The gprs-charging-info parameter contains further parameters: ggsn and gcid. The gcid parameter contains charging identifiers for one or more PDP contexts, or GCID. Each gcid parameter has an identifier assigned by the GGSN (pdp-id parameter), the authorization token used when PDP context was established (auth-token) and an index number (pdpflow-index parameter) to correlate the PDP context with a media stream in the SDP from the SIP signalling. The numbering for the index shall start at 1 and is associated with the 'm' lines in the SDP, where the counting is done from top to bottom.

The GPRS charging information is passed at the first opportunity after the resources are allocated at the GGSN. GPRS charging information will be updated with new information during the session as media streams are added or removed.

4.5.4 Inter operator identifier (IOI)

The Inter Operator Identifier (IOI) is globally unique identifier to share between operator networks/service providers/content providers. There are two possible instances of IOI to be exchanged between networks/service providers/content providers: one for the originating side, ~~ioi-originating~~orig-ioi, and one for the terminating side, ~~ioi-terminating~~term-ioi.

The originating network populates the ~~ioi-originating~~orig-ioi parameter of the P-Charging-Vector header in the initial request, which identifies the operator network from which the request originated. Also in the initial request, the ~~ioi-terminating~~ term-ioi parameter is left out of the P-Charging-Vector parameter. The originating network retrieves the ~~teminating-ioi~~term-ioi parameter from the P-Charging-Vector header within the message sent in response to the initial request, which identifies the operator network from which the response was sent. The MGCF takes responsibility for populating the ~~ioi-originating~~orig-ioi on behalf of the PSTN/PLMN when a call/session is originated from the PSTN/PLMN.

The terminating network retrieves the ~~ioi-originating~~orig-ioi parameter from the P-Charging-Vector header in the initial request, which identifies the operator network from which the request originated. The terminating network populates the ~~ioi-terminating~~term-ioi parameter of the P-Charging-Vector header in the response to the initial request, which identifies the operator network from which the response was sent. IOIs will not be passed along within network. However, IOIs will be sent to AS for accounting purposes.

4.5.5 Charging function addresses

Charging function addresses are distributed to each of the IMS network entities in the home network for one side of the session (either the calling or called side) and are to provide a common location for each entity to send charging information. Charging Collection Function (CCF) addresses are used for offline billing. Event Charging Function (ECF) addresses are used for online billing.

There may be two separate addresses for CCF and ECF addresses populated into the P-Charging-Function-Addresses header of the SIP request or response. The parameters are ccf1~~-primary~~, ccf2~~-secondary~~, ecf1~~-primary~~ and ecf2~~p-secondary~~. Only ccf1~~-primary~~ is required. The other parameters are optional. The secondary addresses may be included by each IMS network for redundancy purposes.

The CCF addresses and ECF addresses are retrieved from HSS via Cx interface and passed by the S-CSCF to subsequent entities. The charging function addresses are passed from the S-CSCF to IM CN subsystem entities in its home network, but are not passed to the visited network or the UE. When the P-CSCF is allocated in the visited network, then the charging function addresses are obtained by means outside the scope of this document. The AS receives the charging function addresses from the S-CSCF via the ISC interface.

End of first changes

Start of second changes

5.2 Procedures at the P-CSCF

5.2.1 General

The P-CSCF shall support the Path and P-Service-Route headers.

NOTE 1: 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 request.

When the P-CSCF sends any request or response to the UE, before sending the message the P-CSCF shall:

- remove the P-Charging-Function-Addresses and P-Charging-Vector headers, if present.

When the P-CSCF receives any request or response from the UE, the P-CSCF shall:

- remove the P-Charging-Function-Addresses and P-Charging-Vector headers, if present. Also, the P-CSCF shall ignore any data received in the P-Charging-Function-Addresses and P-Charging-Vector headers; and

- may insert previously saved values into the P-Charging-Function-Addresses and P-Charging-Vector headers before forwarding the message.

NOTE 2: When the P-CSCF is located in the visited network, then it will not receive the P-Charging-Function-Addresses header from the S-CSCF or I-CSCF. Instead, the P-CSCF discovers charging function addresses by other means not specified in this document.

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) 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

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

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

1) 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.

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

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

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

5.2.3 Subscription to the users registration-state event package

Upon receipt of a 2xx response to the initial REGISTER request of an user, the P-CSCF shall subscribe to the users registration-state event package at the users registrar (S-CSCF) as described in draft-beckmann-sip-reg-event-01 [43]. Therefore the P-CSCF shall generate a SUBSCRIBE request with the following elements:

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

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

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

5.2.4 Registration of multiple public user identites

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

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

- if a registration state value "closed", i.e. deregistered is received for one or more public user identities, the P-CSCF shall release all stored information for these public user identities.

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

5.2.5 Deregistration

5.2.5.1 User-initiated deregistration

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

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

5.2.5.2 Network-initiated deregistration

If the P-CSCF:

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

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

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

5.2.6 General treatment for all dialogs and standalone transactions excluding the REGISTER method

5.2.6.1 Introduction

The procedures of subclause 5.2.6 and its subclauses are general to all requests and responses, except those for the REGISTER method. Procedures in subsequent clauses to subclause 5.2.6 apply in addition to the procedures of subclause 5.2.6.

5.2.6.2 Determination of mobile-originated or mobile-terminated case

Upon receipt of an initial request or a 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.

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:

- remove any Route header from the request;
- 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;
- pre-load the list of Route headers to the request;
- create a Record-Route header containing its own SIP URL;
- insert a P-Asserted-Identity header with a value representing the initiator of the request;
- create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and
- 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:

- store the values received in the P-Charging-Function-Addresses header;
- remove the list of Record-Route headers from the received response;
- 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;
- store the dialog ID and associate it with the private user identity and public user identity involved in the session; and
- save the Contact header received in the response in order to release the dialog if needed.

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

- 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 a refresh request for a dialog, the P-CSCF shall:

- remove any Route header from the request;
- select the list of Route headers that was created during the exchange of the initial request and its associated response;
- pre-load the list of Route headers to the request;
- create a Record-Route header containing its own SIP URL;

- verify if the request relates to a dialog in which the originator of the request is involved. If the request does not relates to a dialog in which the originator is involved, then a 403 response shall be sent back to the originator; and

- 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:

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

- 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; and

- save the Contact header received in the response in order to release the dialog if needed.

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

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

- remove any Route header from the request;

- 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;

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

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

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

- forward the request based on the topmost Route header.

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

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

- 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 request that pertains to an existing dialog, the P-CSCF shall:

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

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

- verify if the request relates to a dialog in which the originator of the request is involved. If the request does not relate to a dialog in which the originator is involved, then a 403 response shall be sent back to the originator; and

- forward the request based on the topmost Route header.

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

- verify if the request relates to a dialog in which the originator of the request is involved.. If the request does not relates to a dialog in which the originator is involved, then a 403 response shall be sent back to the originator; and

- remove any list of Record-Route headers, valid or not, from the received response and forward it to the UE.

When the P-CSCF receives from the UE an initial request for a dialog, a 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:

- 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:

- 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;
- pre-load the list of Route headers to the request,
- insert an P-Asserted-Identity header with a value representing the initiator of the request; and
- forward the request based on the topmost Route header.

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

- remove any list of Record-Route headers, even though invalid, from the received response and forward it to the UE.

~~When the P-CSCF receives any request or response from the UE, the P-CSCF shall:~~

- ~~remove the <charging-vector> XML element (see subclause 7.6), if present, from the message body of the received request or response.~~

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 refresh request for a dialog, prior to forwarding the request, the P-CSCF shall:

- remove its own SIP URL from the topmost Route header;
- 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;
- save the Contact header received in the response in order to release the dialog if needed;
- 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;
- 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;
- store the values received in the P-Charging-Function-Addresses header; and
- 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:

- insert an P-Asserted-Identity header with a value representing the responder to the request;
- append the saved list of Record-Route headers to the response;

- append the saved list of Via headers to the response; and
- 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:

- 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:

- insert an P-Asserted-Identity header with a value representing the responder to the request;
- 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;
- store the values received in the P-Charging-Function-Addresses header; and
- 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:

- append the saved list of Via headers to the response; and
- verify if the request relates to a dialog in which the originator of the request is involved. If the request does not relate to a dialog in which the originator is involved, then a 403 response shall be sent back to the originator.

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

- 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
- remove and store the icid parameter from P-Charging ~~Identity~~ Vector header ~~(see subclause 7.6)~~.

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

- append the saved list of Via headers to the response.

~~When the P-CSCF sends any request or response to the UE, the P-CSCF shall:~~

- ~~remove the P-Charging-Vector header from the request or response.~~

End of second changes

Start of third changes

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 P-Original-Dialog-ID header is present in the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The od-to-tag, od-from-tag and od-call-idparameter values from the P-Original-Dialog-ID header may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the P-Original-Dialog-ID header in the request. If the next hop is not an Application Server, the S-CSCF shall remove the P-Original-Dialog-ID header from the request;

- check whether the initial request matches the initial filter criteria, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

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

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

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

- insert an ~~ioi-originating~~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 ~~ioi-originating~~orig-ioi parameter shall be set to a value that identifies the sending network. The ~~ioi-terminating~~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 refresh request for a dialog, prior to forwarding the request the S-CSCF shall:

- remove its own URL from the topmost Route header;

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

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

- route the request based on the topmost Route header.

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

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

- remove its own URL from the topmost Route header;

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

- route the request based on the topmost Route header.

5.4.3.3 Requests terminated at the served user

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

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

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

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

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

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

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

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

6) store the value of the ~~ioi-originating~~orig-ioi parameter received in the P-Charging-Vector header, if present. The ~~ioi-originating~~orig-ioi parameter identifies the sending network of the request message. The ~~ioi-originating~~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;

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

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

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

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

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

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

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

5.4.3.4 Original dialog identifier

The original dialog identifier is coded as the P-Original-Dialog-ID as described in subclause 7.2.7.

5.4.3.5 Abnormal cases

The S-CSCF shall, when contacting application servers based on the initial filter criteria, expect either a final response from the application server as the session terminates there, or the initial request message, that may be modified. In either case the message should be identified (using P-Original-Dialog-ID) as belonging to the original request forwarded by the S-CSCF.

If the S-CSCF receives a message including an P-Original-Dialog-ID that does not match any that it has forwarded to the application server it shall:

- respond to the application server with 481 Call Leg/Transaction Does Not Exist.

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 ~~ioi-terminating~~term-ioi parameter received in the P-Charging-Vector header, if present. The ~~ioi-terminating~~term-ioi parameter identifies the sending network of the response message. The ~~ioi-terminating~~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 ~~ioi-terminating~~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 ~~ioi-terminating~~term-ioi parameter shall be set to a value that identifies the sending network of the response and the ~~ioi-originating~~orig-ioi parameter is set to the previously received value of ~~ioi-originating~~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.

End of third changes

Start of fourth changes

5.5 Procedures at the MGCF

5.5.1 General

The MGCF, 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. Therefore the dependencies of table A.3/1 and table A.3/2 shall not apply.

The use of the Path and P-Service-Route headers shall not be supported by the MGCF.

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

5.5.2 Subscription and notification

Void.

5.5.3 Call initiation

5.5.3.1 Initial INVITE

5.5.3.1.1 Calls originated from circuit-switched networks

When the MGCF receives an indication of an incoming call from a circuit-switched network, the MGCF shall:

- generate and send an INVITE request to I-CSCF:
  - set the Request-URI to the "tel" format using an E.164 address;
  - set the Supported header to "100rel" (see RFC 3312 [30]);
  - include an P-Asserted-Identity header;
  - create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and
  - insert an ~~ioi originating~~orig-ioi parameter into the P-Charging-Vector header. The ~~ioi originating~~orig-ioi parameter shall be set to a value that identifies the sending circuit-switched network and the ~~ioi terminating~~term-ioi parameter shall not be included.

5.5.3.1.2 Calls terminating in circuit-switched networks

When the MGCF receives an initial INVITE request with Supported header indicating "100rel", the MGCF shall:

- send 100 (Trying) response;
- after a matching codec is found at the MGW, send 183 "Session Progress" response:
  - set the Require header to the value of "100rel";
  - set the Content-Disposition header to the value of "precondition";
  - include an P-Asserted-Identity header; and
  - store the values received in the P-Charging-Function-Addresses header; and
  - store the value of the icid parameter received in the P-Charging-Vector header.

When the MGCF does not find an available matching codec at the MGW for the received initial INVITE request, the MGCF shall:

- send 503 (Service Unavailable) response if the type of codec was acceptable but none were available; or
- send 488 (Not Acceptable Here) response if the type of codec was not supported, and may include SDP in the message body to indicate the codecs supported by the MGCF/MGW.

5.5.3.2 Subsequent requests

5.5.3.2.1 Calls originating in circuit-switched networks

When the MGCF receives 183 response to an INVITE request, the MGCF shall:

- store the values received in the P-Charging-Function-Addresses header.

When the MGCF receives 200 (OK) response to a PRACK request and notification that bearer setup is complete, the MGCF shall:

- send an UPDATE request.

5.5.3.2.2 Calls terminating in circuit-switched networks

When the MGCF receives an indication of a ringing for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 180 Ringing to the UE.

When the MGCF receives an indication of answer for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 200 OK to the UE, including an P-Asserted-Identity header.

End of fourth changes

Start of fifth changes

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.

5.7.2 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.

The S-CSCF may forward received initial requests to the application server based on initial filter criteria being met. If the S-CSCF includes P-Original-Dialog-ID header in these requests, the AS shall include the same P-Original-Dialog-ID header in any responses and/or subsequent requests sent on this dialog.

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

The S-CSCF may forward received initial requests to the application server based on initial filter criteria being met. If the S-CSCF includes P-Original-Dialog-ID header in these requests, the AS shall include the same P-Original-Dialog-ID header in any responses and/or subsequent requests sent on this dialog.

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. The AS shall look for the presence of the P-Original-Dialog-ID header in the initial INVITE request and populate the same P-Original-Dialog-ID header in the new INVITE request;

- 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> XML element~~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.

End of fifth changes

Start of sixth changes

7.2.5 P-Charging-Function-Addresses header

7.2.5.1 Introduction

The P-Charging-Function-Addresses header is the mechanism whereby the S-CSCF may distribute a common set of addresses for charging functions to other network entities within the same network as the S-CSCF. The primary Charging Correlation Function (~~CCF~~ccf1) address is a required parameter for offline charging. The secondary CCF address is optional (ccf2). Both the primary and secondary Event Charging Function (~~ECF~~ecf1 and ecf2) addresses for online charging are optional.

The S-CSCF inserts the header at the first opportunity when initialising dialogs and with standalone transactions. The header may be included in requests and responses.

7.2.5.2 Syntax

The P-Charging-Function-Addresses header field has the syntax described in draft-henrikson-sip-charging-information [45].

7.2.5.3 Operation

The operation of this header is described in subclauses 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8.

7.2.6 P-Charging-Vector header

7.2.6.1 Introduction

The P-Charging-Vector header is the mechanism whereby the charging correlation information may be shared by IM CN subsystem functional entities. The charging correlation information consists of the following:

- IMS Charging Identifier (ICID), which is a globally unique identifier created per IMS dialog that is stored in all related CDRs.
- Inter Operator Identifier (IOI), which are globally unique identifiers for a particular network.
- Access Network Charging Information, where the GPRS is the initially supported access network. For GPRS there are the following components to track: GGSN address and one or more GPRS Charging Identifiers (GCID). Each GCID consists of an identifier of the PDP context assigned, the associated flow index into the SDP from the SIP signalling and the authorization token associated with the PDP context.

The first IM CN subsystem functional entity involved with a dialog or standalone transaction inserts the header with the icid parameter. Additional parameters are inserted into the P-Charging-Vector header by other entities as the processing continues. The header may be included in requests and responses.

7.2.6.2 Syntax

The P-Charging-Vector header field has the syntax described in table 7.3, which is extracted from draft-henrikson-sip-charging-information [45]. Table 7.3 describes extensions required for 3GPP.

Table 7.3: Syntax of extensions to P-Charging-Vector header

```
access-network-charging-info = (gprs-charging-info / gen-value)
gprs-charging-info = "gprs-charging-info" SEMI
                     "ggsn" EQUAL ggsn *(SEMI "gcid" EQUAL gcid)
                     [COMMA extension-param]
ggsn = gen-value
gcid = "pdp-id" EQUAL pdp-id COMMA "flow-index" EQUAL flow-index
       COMMA "auth-token" EQUAL auth-token
pdp-id = gen-value
flow-index = gen-value
auth-token = gen-value
extension-param = token [EQUAL (token | quoted-string)]
```

The gprs-charging-info parameter contains one ggsn child parameter and one or more child gcid parameters. Each gcid child parameter within gprs-charging-info corresponds to a PDP context that was established at the GGSN for a UE. Each gcid parameter contains pdp-id, flow-index and auth-token child parameters. The pdp-id parameter is the PDP context identifier that the P-CSCF obtained from the GGSN. The flow-index parameter is the relative index to the media stream in the SDP for the PDP context. The auth-token parameter is the authorization token associated with the PDP context. For more information about the PDP contexts for media, see subclause 9.2.5. For the case of a primary PDP context that is used for signalling, the flow-id and auth-token parameters are set to 0.

7.2.6.3 Operation

The operation of this header is described in subclauses 5.2, 5.3, 5.4, 5.5, 5.6, 5.7 and 5.8.

End of sixth changes

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

Tdoc N1-021797

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **143** ⌘ **rev** **1** ⌘ Current version: **5.1.0** ⌘

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

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

Title:	⌘	Replace P-Original-Dialog-ID header with unique data in Route header
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	July 30, 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 internet draft for P-Original-Dialog-ID is not going forward. An alternative was identified to use a unique user part (of a SIP URI or SIPS URI) in a Route header that is generated and looked at by the S-CSCF. The alternative does not require any changes to SIP.
Summary of change:	⌘	The references to P-Original-Dialog-ID are removed. The locations where it is used are replaced with a description of how a Route header may be inserted by the S-CSCF with a unique user part that will be returned to the S-CSCF by the AS. The S-CSCF will use this to make the association with the previous dialog.
Consequences if not approved:	⌘	24.229 will be referencing a P-header for an internet draft that is not progressing towards RFC (standards) status.

Clauses affected:	⌘	2, 5.4.3, 5.7.2, 5.7.4, 5.7.5, 7.2.7

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

Other comments:	⌘	Revision1 incorporates modification requested by Ericsson pertaining to using the user-part in URL (for original dialog ID). It indicates that other parameters in the URL may also be used. In addition, the editorial changes requested by Dynamicsoft are included, and the term “vendor specific” has been replaced with “implementation specific.”

How to create CRs using this form:

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

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

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

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

Start of First Change

2 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

End of First Change

Start of Second Change

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 ~~P-Original-Dialog-ID header~~an original dialog identifier that the S-CSCF previously placed in a Route header ~~is~~ is present in the ~~user part of 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~~. The od-to-tag, od-from-tag and od-call-idparameter values from the P-Original-Dialog-ID header may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the P-Original-Dialog-ID~~

~~header in the request. If the next hop is not an Application Server, the S-CSCF shall remove the P-Original-Dialog-ID header from the request~~;

- check whether the initial request matches the initial filter criteria, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

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

  - ~~populate the P-Original-Dialog-Id~~user part of the Route ~~header that has its own URL in the message with the original dialog identifier To tag, From tag and Call-ID headers received in the request. See subclause 7.2.7~~5.4.3.4 ~~for further information on the original dialog identifier;~~

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

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

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

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

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

- determine the destination address (e.g. DNS access) using the URL placed in the topmost Route header if present, otherwise based on the Request-URI;

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

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

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

- route the request based on SIP routeing procedures.

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

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

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

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

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

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

- remove its own URL from the topmost Route header;

- create a Record-Route header containing its own SIP URL and save the Contact header from the request in order to release the dialog when needed;
- remove the P-Access-Network-Info header and act upon the contents accordingly; and
- route the request based on the topmost Route header.

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

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

- remove its own URL from the topmost Route header;
- remove the P-Access-Network-Info header and act upon the contents accordingly; and
- route the request based on the topmost Route header.

5.4.3.3 Requests terminated at the served user

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

1) remove its own URL from the topmost Route header;
2) check if ~~P-Original-Dialog-ID header~~ an original dialog identifier that the S-CSCF previously placed in a Route header is present in the ~~user part of 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~~. The od-to-tag, od-from-tag and od-call-id parameter values from the P-Original-Dialog-ID header may be used as additional parameters when searching for existing dialogs. The S-CSCF shall determine the next hop using initial filter criteria. If the next hop is another Application Server, the S-CSCF shall retain the P-Original-Dialog-ID header in the message of the request. If the next hop is not an Application Server, the S-CSCF shall remove the P-Original-Dialog-ID header from the request~~;
3) check whether the initial request matches the initial filter criteria, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:
   a) insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL populated as specified in the subclause 5.4.3.4; ~~and~~
   b) ~~populate the P-Original-Dialog-ID user part of the Route header that has its own URL in the message with the original dialog identifierTo tag, From tag and Call-ID headers received in the request. See subclause 5.4.3.4 for further information on the original dialog identifier;~~
4) insert a P-Charging-Function-Addresses header (see subclause 7.2.4) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;
5) store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header;
6) store the value of the ioi-originating parameter received in the P-Charging-Vector header, if present. The ioi-originating parameter identifies the sending network of the request message. The ioi-originating parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS;
7) in case there are no Route headers in the request, then determine, from the destination public user identity, the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2;
8) build the Route header field with the values determined in the previous step;

9) determine, from the destination public user identity, the saved Contact URL where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.4.3.4 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.

~~The coding of the original dialog identifier in the user part (a component of SIP URI or SIPS URI) of the Route header is vendor specific. This is possible because the S-CSCF is the only entity that creates and consumes the value. 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 is coded as the P-Original-Dialog-ID as described in subclause 7.2.7.~~

5.4.3.5 Void~~Abnormal cases~~

~~The S-CSCF shall, when contacting application servers based on the initial filter criteria, expect either a final response from the application server as the session terminates there, or the initial request message, that may be modified. In either case the message should be identified (using P-Original-Dialog-Id) as belonging to the original request forwarded by the S-CSCF.~~

~~If the S-CSCF receives a message including an P-Original-Dialog-ID that does not match any that it has forwarded to the application server it shall:~~

- ~~respond to the application server with 481 Call Leg/Transaction Does Not Exist.~~

End of Second Change

Start of Third 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.

5.7.2 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.

~~The S-CSCF may forward received initial requests to the application server based on initial filter criteria being met. If the S-CSCF includes P-Original-Dialog-ID header in these requests, the AS shall include the same P-Original-Dialog-ID header in any responses and/or subsequent requests sent on this dialog.~~

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

~~The S-CSCF may forward received initial requests to the application server based on initial filter criteria being met. If the S-CSCF includes P-Original-Dialog-ID header in these requests, the AS shall include the same P-Original-Dialog-ID header in any responses and/or subsequent requests sent on this dialog.~~

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~~. The AS shall look for the presence of the P-Original-Dialog-ID header in the initial INVITE request and populate the same P-Original-Dialog-ID header in the new INVITE request~~;
- 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> XML element 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.

End of Third Change

Start of Fourth Change

7.2.7 ~~P-Original-Dialog-ID header~~Void

~~7.2.7.1 Introduction~~

~~The P-Original-Dialog-ID header is the mechanism whereby the S-CSCF may associate dialogs related to the same initial request when traversing Application Servers specified in filter criteria.~~

~~The S-CSCF inserts the header in all INVITE and reINVITE requests. The header may also be used with standalone transactions and included in responses.~~

~~7.2.7.2 Syntax~~

~~The P-Original-Dialog-ID header field has the syntax described in draft-henrikson-sip-original-dialog-id [46].~~

~~7.2.7.3 Operation~~

~~The operation of this header is described in subclauses 5.4.3, 5.7.2, 5.7.4 and 5.7.5.~~

End of Fourth Change

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

Tdoc N1-021812

CR-Form-v7

CHANGE REQUEST

⌘ **TS 24.229** **CR** **140** ⌘ **rev** **1** ⌘ Current version: **5.1.0** ⌘

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

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

Title:	⌘	Support of non-IMS forking
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	31/07/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

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

Use one of the following releases:

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

Reason for change:	⌘	Align with SA2 which documented in 23.228 how IMS should support forking done externally to the IMS network.
Summary of change:	⌘	Changes to UE, P-CSCF, I-CSCF and S-CSCF procedures to handle forking.
Consequences if not approved:	⌘	Misalignment with SA2

Clauses affected:	⌘	4.1, new clause 5.1.x			
Other specs affected:	⌘	**Y** / **N**	Other core specifications	⌘	29.207, 27.060
		[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

4.1 Conformance of IM CN subsystem entities to SIP

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

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

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

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

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

3GPP IM CN subsystem SIP proxies (i.e., P-CSCF, I-CSCF, S-CSCF, BGCF and AS) of this specification do not initiate forking of SIP requests, but shall be prepared to react to non-IMS upstream or downstream forking.

- The User Equipment (UE) shall provide the User Agent (UA) rolewith the exceptions and additional capabilities as described in subclause 5.1.
- The P-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.2. When acting as the subscriber to or the recipient of event information, the P-CSCF shall provide the UA role, again with the exceptions and additional capabilities as described in subclause 5.2.
- The I-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.3.
- The S-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.4. Under certain circumstances as described in subclause 5.4, the S-CSCF shall provide the UA role with the additional capabilities, as follows:

  a) the S-CSCF shall also act as a registrar. When acting as a registrar, or for the purposes of executing a third-party registration, the S-CSCF shall provide the UA role;

  b) as the notifier of event information the S-CSCF shall provide the UA role; and

  c) when performing S-CSCF initiated release the S-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.
- The BGCF shall provided the proxy role, with the exceptions and additional capabilities as described in subclause 5.5.
- The MGCF shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.6.

- The AS, acting as terminating UA, or redirect server (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.1), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.2.

- The AS, acting as originating UA (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.2), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.3.

- The AS, acting as a SIP proxy (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.3), shall provided the proxy role, with the exceptions and additional capabilities as described in subclause 5.7.4.

- The AS, performing 3rd party call control (as defined in 3GPP TS 23.218 [5] subclause 9.1.1.4), shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.7.5.

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

- The MRFC shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.8.

NOTE: The allocated roles defined in this clause are the starting point of the requirements from the IETF SIP specifications, and are then the basis for the description of further requirements. Some of these extra requirements formally change the proxy role into a B2BUA. Thus, for example, a P-CSCF is a B2BUA in that it inspects and may modify SDP message bodies, and terminates Record-Route headers on behalf of the UA, but in all other respects other than those more completely described in subclause 5.2 it implements proxy requirements. Despite being a B2BUA a P-CSCF does not implement UA requirements from the IETF RFCs, except as indicated in this specification, e.g., relating to registration event subscription.

Next proposed change

5 Application usage of SIP

5.1 Procedures at the UE

5.1.x Support for forking

~~This subclause describes the actions required at the UE in order to support non-IMS forking. Forking affects the UE when it acts as a UAC or as a UAS.~~

5.1.x.1 UE acting as UAS

~~When the UE is acting as a UAS, t~~The UE shall be able to receive several forked requests for the same transaction. These request are similar, except for the branch parameter value present in the Via header value. If the first forked request was accepted and answered with a 200 (OK) response, then the subsequent requests shall be answered with a 482 (Loop detected) response.

5.1.x.1 UE acting as UAC

~~When the UE is acting as a UAC, t~~The UE shall be able to receive several forked provisional or final responses from different terminations. The UE may accept or reject the forked responses. For example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs, when the number of provisional responses exceeds the limit, it ~~can~~may reject newer ones by sending a BYE request. .

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

1) ~~T~~the bearer requirements of the subsequent SDP can be accommodated by the existing PDP context(s). No activation/modification of PDP contexts is performed.

2) ~~T~~the subsequent SDP introduces~~requires increased~~ different QoS requirements or additional IP flows. These ~~that~~ are accommodated by modification of the existing PDP context(s) according to subclause 9.2.5.

3) ~~T~~the subsequent SDP introduces one or more additional IP flows. These ~~that~~ are accommodated by establishing additional PDP context(s) according to subclause 9.2.5.

4) the subsequent SDP introduces requirements to separate in different PDP contexts some media streams that were previously allowed to be combined in a single PDP context. In this case, the UE shall separate the media streams, unless separate PDP contexts are already in place, as indicated by the P-CSCF. This may require a modification of the existing PDP contexts and/or establishment of additional PDP contexts according to subclause 9.2.5.~~The P-CSCF indicates to the UE in the subsequent provisional response that an IP flow(s) already combined with other flows in an existing PDP context must use a dedicated PDP context. The flow(s) must be removed from the existing PDP context to avoid double booking of resources for the actual flow according to the procedures for revoke decision in [12]. A new PDP context is established for the separated flow. The UE may rearrange the flows to PDP contexts according to subclause 9.2.5 for other reasons also.~~

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

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

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. Any further provisional or final answers received by the UE shall not progress the early dialogues to established dialogs. All the remaining early dialogues shall be terminated and the related radio/bearer resources are released.

Upon the reception of a first final 200 (OK) response for INVITE, the UE shall:

1) acknowledge the response with an ACK request;

2) keep the early dialogues alived for 64*T1 seconds, in the event a new 200 (OK) response arrives, according to the procedures described in RFC 3261 [26] section 13.2.2.4, and;

3) in case PDP context(s) were established or modified as a consequence of the INVITE and forked provisional responses that are not related to the accepted 200 (OK) response, the PDP context(s) shall be deleted or modified back to their original state;

~~- delete the PDP contexts established as a consequence of the INVITE and forked provisional responses that are not related to the accepted 200 (OK) response;~~

Upon the reception of a subsequent final 200 (OK) response for INVITE, the UE shall:

1) acknowledge the response with an ACK request; and

2) send a BYE request to this dialog in order to terminate it

~~received by the UE shall not progress the early dialogues to established dialogsAll the remaining;~~

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

Tdoc N1-~~021559~~021814

CR-Form-v7

CHANGE REQUEST

⌘ **TS 24.229** **CR** **141** ⌘ **rev** **1** ⌘ Current version: **5.1.0** ⌘

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

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

Title:	⌘	Adding MESSAGE to 24.229
Source:	⌘	Ericsson, dynamicsoft, Nortel, Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	02/08/2002
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:	⌘	Align with SA2's 23.228 which documents the capabilities that an IM CN susbsytems can be used to conduct session-unrelated and session unrelated MESSAGE interactions between: 1) users, 2) S-CSCF & users, 3) AS & users.
Summary of change:	⌘	Add MESSAGE in 24.229 R5 to support that SA2 capability.
Consequences if not approved:	⌘	Functional misalignment with SA2.

Clauses affected:	⌘	2, 5.1.1.2, 5.1.x, 5.2.x, 5.3.x, 5.4.1.2.1, 5.4.x, 5.7.x, A.2.1.2, A.2.1.3, A.2.1.4.x

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

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

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

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

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

2 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[48] draft-ietf-sip-message-06.txt (July 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.

[49] 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.

5 Application usage of SIP

5.1 Procedures at the UE

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 [48], and in the Caller Preferences draft-ietf-sip-callerprefs-06.txt [49].

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

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

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

b) the From header shall contain the public user identity to be registered;

c) the To header shall contain the public user identity to be registered;

d) the Expires header, or the expires parameter within the Contact header, shall contain 600 000 seconds as the value desired for the duration of the registration; and

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

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

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

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

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

On receiving the 200 (OK) response to the REGISTER request, the UE shall store the expiration time of the registration for the public user identities found in the To header value. The UE shall also store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving a 423 (Interval Too Brief) too brief response to the REGISTER request, the UE shall:

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

5.1.x MESSAGE support

The UE shall support the SIP MESSAGE method described in draft-ietf-sip-message-06 [48]. A UE shall be capable of sending and receiving MESSAGE method to conduct session-unrelated or session-related interactions. To do so, a UE may either initiate or terminate MESSAGE requests per draft-ietf-sip-message-06.txt [48]. The UE should support, as a minimum, a body of type “text/plain” per draft-ietf-sip-message-06.txt [48].

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

5.2 Procedures at the P-CSCF

5.2.x MESSAGE support

If the P-CSCF proxies a SIP MESSAGE request which size exceeds 1300 bytes (before applying any compression), the P-CSCF shall use TCP transport protocol for sending the MESSAGE request.

5.3 Procedures at the I-CSCF

5.3.x MESSAGE support

If the I-CSCF proxies a SIP MESSAGE request which size exceeds 1300 bytes, the I-CSCF shall use TCP transport protocol for sending the MESSAGE request.

5.4 Procedures at the S-CSCF

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Initial registration

Upon receipt of a REGISTER request for a user that is not registered and for which also no authentication is currently ongoing (i.e. timer reg-await-auth is not running), 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;

4) 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 1: 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.

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

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

7) 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) send the so generated 401 (Unauthorized) response towards the UE; and,

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

While timer reg-await-auth is running, upon receipt of a REGISTER request, 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) stop timer reg-await-auth;

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

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 of the user including initial Filter Criteria;

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 adjust the duration of the registration due to local policy;

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) 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, according to the local policy of the network, if this expiration time is shorter than the requested expiry time received from the UE; 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) send the so created 200 (OK) response to the UE;

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

5.4.x 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 [48]. The S-CSCF should support, as a minimum, a body of type “text/plain” per draft-ietf-sip-message-06.txt [48].

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.

5.7 Procedures at the Application Server (AS)

5.7.x 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 [48]. The AS should support, as a minimum, a body of type “text/plain” per draft-ietf-sip-message-06.txt [48].

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.

Annex A (normative): Profiles of IETF RFCs for 3GPP usage

A.2 Profile definition for the Session Initiation Protocol as used in the present document

A.2.1.2 Major capabilities

Table A.4: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
1	client behaviour for registration?	[26] subclause 10.2	m	c3
2	registrar?	[26] subclause 10.3	o	c4
3	client behaviour for session requests?	[26] subclause 13.2	m	o
4	server behaviour for session requests?	[26] subclause 13.3	m	o
5	session release?	[26] subclause 15.1	m	c1
6	timestamping of requests?	[26] subclause 8.2.6.1	o	o
7	authentication between UA and UA?	[26] subclause 22.2	o	o
8	authentication between UA and registrar?	[26] subclause 22.2	o	n/a
9	server handling of merged requests due to forking	[26] 8.2.2.2	m	m
10	client handling of multiple responses due to forking	[26] 13.2.2.4	m	m
11	insertion of date in requests and responses?	[26] subclause 20.17	o	o
12	downloading of alerting information?	[26] subclause 20.4	o	o
	Extensions			
13	The SIP INFO method?	[25]	o	n/a
14	Reliability of provisional responses in SIP?	[27]	o	m
15	the REFER method?	[36]	o	o
16	Integration of resource management and SIP?	[30]	o	m
17	the SIP UPDATE method	[29]	c5	m
18	SIP extensions for caller identity and privacy?	[34]	o	m
19	SIP extensions for media authorization?	[31]	o	m
20	SIP specific event notification	[28]	o	o
21	the use of NOTIFY to establish a dialog	[28] 4.2	o	n/a
22	acting as the notifier of event information	[28]	c2	c2
23	acting as the recipient of event information	[28]	c2	c2
24	Path Extension Header for Establishing Service Route with SIP REGISTER	[35]	o	c6
25	extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks	[34]	o	m
26	a Privacy Mechanism for the Session Initiation Protocol (SIP)	[33]	o	m
27	A messaging mechanism for the Session Initiation Protocol (SIP)	[48]	o	m

c1:	IF A.4/3 OR A.4/4 THEN m ELSE o.
c2:	IF A.4/20 THEN o.1 ELSE n/a.
c3:	IF A.3/1 OR A.3/4 THEN m ELSE n/a - - UA or S-CSCF functional entity.
c4:	IF A.3/4 OR A.3/7 THEN m ELSE n/a - - S-CSCF or AS functional entity.
c5:	IF A.4/16 THEN m ELSE o - - integration of resource management and SIP.
c6:	IF (A.150/3 AND A.150/4) THEN m ELSE n/a. - - S-CSCF acting as registrar.
o.1:	At least one of these capabilities is supported.

A.2.1.3 PDUs

Table A.5: Supported methods

Item	PDU	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	ACK request	[26] 13	m	m	[26] 13	m	m
2	BYE request	[26] 15.1	o		[26] 15.1	o	
3	BYE response	[26] 15.1	o		[26] 15.1	o	
4	CANCEL request	[26] 9	o		[26] 9	o	
5	CANCEL response	[26] 9	o		[26] 9	o	
6	INFO request	[25] 2	c2	n/a	[25] 2	c2	n/a
7	INFO response	[25] 2	c2	n/a	[25] 2	c2	n/a
8	INVITE request	[26] 13	m	m	[26] 13	m	m
9	INVITE response	[26] 13	m	m	[26] 13	m	m
10	NOTIFY request	[28] 8.1.2	c4	c4	[28] 8.1.2	c3	c3
11	NOTIFY response	[28] 8.1.2	c3	c3	[28] 8.1.2	c4	c4
12	OPTIONS request	[26] 11	m	m	[26] 11	m	m
13	OPTIONS response	[26] 11	m	m	[26] 11	m	m
14	PRACK request	[27] 6	c5	c5	[27] 6	c5	c5
15	PRACK response	[27] 6	c5	c5	[27] 6	c5	c5
16	REFER request	[36] 3	c1	c1	[36] 3	c1	c1
17	REFER response	[36] 3	c1	c1	[36] 3	c1	c1
18	REGISTER request	[26] 10	o		[26] 10	n/a	
19	REGISTER response	[26] 10	n/a		[26] 10	m	
20	SUBSCRIBE request	[28] 8.1.1	c3	c3	[28] 8.1.1	c4	c4
21	SUBSCRIBE response	[28] 8.1.1	c4	c4	[28] 8.1.1	c3	c3
22	UPDATE request	[30] 6.1	c6	c6	[30] 6.2	c6	c6
23	UPDATE response	[30] 6.2	c6	c6	[30] 6.1	c6	c6
24	MESSAGE request	[48] 4	c7	c7	[48] 7	c7	c7
25	MESSAGE response	[48] 4	c7	c7	[48] 7	c7	c7
c1:	IF A.4/15 THEN m ELSE n/a.						
c2:	IF A.4/13 THEN m ELSE n/a.						
c3:	IF A.4/23 THEN m ELSE n/a.						
c4:	IF A.4/22 THEN m ELSE n/a.						
c5:	IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses.						
c6:	IF A.4/17 THEN m ELSE n/a - - the SIP update method.						
c7:	IF A.4/27 THEN m ELSE n/a - - the SIP MESSAGE method.						

A.2.1.4 PDU parameters

A.2.1.4.X MESSAGE method

Prerequisite A.5/24 – MESSAGE request

Table A.xxx: Supported headers within the MESSAGE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[48] 10	m		[48] 10	m	
2	Accept-Encoding	[48] 10	m		[48] 10	m	
3	Accept-Language	[48] 10	m		[48] 10	m	
4	Alert-Info	[48] 10	-		[48] 10	-	
5	Allow	[48] 10	o		[48] 10	m	
6	Allow-Events	[48] 10	n/a		[48] 10	n/a	
7	Anonymity	[48] 10	n/a		[48] 10	n/a	
xxx	Authentication-Info	[48] 10	o		[48] 10	o	
8	Authorization	[48] 10	o		[48] 10	o	
9	Call-ID	[48] 10	m		[48] 10	m	
10	Call-Info	[48] 10	o		[48] 10	o	
11	Contact	[48] 10	o		[48] 10	o	
12	Content-Disposition	[48] 10	o		[48] 10	o	
13	Content-Encoding	[48] 10	o		[48] 10	o	
14	Content-Language	[48] 10	o		[48] 10	o	
15	Content-Length	[48] 10	t		[48] 10	t	
16	Content-Type	[48] 10	*		[48] 10	*	
17	Cseq	[48] 10	m		[48] 10	m	
18	Date	[48] 10	o		[48] 10	o	
19	Expires	[48] 10			[48] 10		
Xxx	Error-Info	[48] 10	o		[48] 10	o	
xxx	Expires	[48] 10	o		[48] 10	o	
20	From	[48] 10	m		[48] 10	m	
21	In-Reply-To	[48] 10	o		[48] 10	o	
22	Max-Forwards	[48] 10	m		[48] 10	m	
23	MIME-Version	[48] 10	-		[48] 10	-	
24	Organization	[48] 10	o		[48] 10	o	
25	P-Media-Authorization	[48] 10	n/a		[48] 10	n/a	
26	Priority	[48] 10	o		[48] 10	o	
27	Proxy-Authorization	[48] 10	o		[48] 10	o	
28	Proxy-Require	[48] 10	o		[48] 10	o	
29	Record-Route	[48] 10	-		[48] 10	-	
30	Remote-Party-ID	[48] 10	n/a		[48] 10	n/a	
31	Reply-To	[48] 10	o		[48] 10	o	
32	Require	[48] 10	c		[48] 10	c	
xxx	Retry-After	[48] 10	o		[48] 10	o	
33	Route	[48] 10	o		[48] 10	o	
xxx	Server	[48] 10	o		[48] 10	o	
34	Subject	[48] 10	o		[48] 10	o	
35	Supported	[48] 10	n/a		[48] 10	n/a	
36	Timestamp	[48] 10	o		[48] 10	o	
37	To	[48] 10	m		[48] 10	m	
xxx	Unsupported	[48] 10	o		[48] 10	o	
38	User-Agent	[48] 10	o		[48] 10	o	
39	Via	[48] 10	m		[48] 10	m	
xxx	Warning	[48] 10	m		[48] 10	m	
xxx	WWW-Authenticate	[48] 10	o		[48] 10	o	

Start of first changes

5.1.2 Subscription and notification

5.1.2.1 Notification about multiple registered public user identities

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

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

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

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

End of first changes

Start of second changes

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.

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Initial registration

Upon receipt of a REGISTER request for a user that is not registered and for which also no authentication is currently ongoing (i.e. timer reg-await-auth is not running), 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;

4) 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 1: 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.

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

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

7) 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) send the so generated 401 (Unauthorized) response towards the UE; and,

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

While timer reg-await-auth is running, upon receipt of a REGISTER request, 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) stop timer reg-await-auth;

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

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 2: 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;

NOTE ~~2~~3:There might be more then one contact information available for one public user identity.

NOTE ~~3~~4: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~~5: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 adjust the duration of the registration due to local policy;

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) 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, according to the local policy of the network, if this expiration time is shorter than the requested expiry time received from the UE; 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) send the so created 200 (OK) response to the UE;

14) 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~~6:If this registration is a reregistration, the Filter Criteria already exists in the local data.

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

5.4.1.2.2 User-initiated reregistration

Upon receipt of a REGISTER request for an already registered 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 From header of the REGISTER request;

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

3) 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;

4) 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

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

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:

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

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

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

5.4.1.5 Network-initiated deregistration

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

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

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

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

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

The S-CSCF shall then deregister the public user identity together with the implicitly registered public user identities.

5.4.1.6 Network-initiated reauthentication

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

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

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

- set the Event header to the "registration-state" value; and

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

Afterwards the S-CSCF shall:

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

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

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

When generating the NOTIFY request, the S-CSCF shall shorten the validity of subscriber's registration timer to an operator defined value that will allow the user to be re-authenticated. If user fails to reauthenticate while its registration is still valid, the S-CSCF shall deregister the private user identity as described in subclause 5.4.1.5 and terminate the ongoing sessions of that user.

5.4.1.7 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 the public user identity as contained in the REGISTER request received form the UE;

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 registration-state event package, the S-CSCF shall generate a 2xx response acknowledging the SUBSCRIBE request and indicating that the subscription was successful. Furthermore, the response shall include:

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

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

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

5.4.2.1.2 Notification about registration state

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

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

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

- set the Event header to the "registration-state" value;

- indicate registration state "open" for all public user identities which are currently registered;

- indicate registration state "closed" for all public user identities which are currently deregistered; and

- indicate within the "<note>" information of those public user identities which will be automatically reregistered the "automatically by" information, followed by the specific public user identity which will cover the reregistration.

EXAMPLE: If sip:user1_public1@home1.net is 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:

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

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

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

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 P-Original-Dialog-ID header is present in the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The od-to-tag, od-from-tag and od-call-idparameter values from the P-Original-Dialog-ID header may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the P-Original-Dialog-ID header in the request. If the next hop is not an Application Server, the S-CSCF shall remove the P-Original-Dialog-ID header from the request;

- check whether the initial request matches the initial filter criteria based on a public user identity in the P-Asserted-Identity header~~from the service profile associated with the received public user identity~~, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

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

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

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

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

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

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

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

- determine the destination address (e.g. DNS access) using the URL placed in the topmost Route header if present, otherwise based on the Request-URI;

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

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

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

- route the request based on SIP routeing procedures.

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

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

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

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

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

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the Contact header from the request in order to release the dialog when needed;
- remove the P-Access-Network-Info header and act upon the contents accordingly; and
- route the request based on the topmost Route header.

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

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

- remove its own URL from the topmost Route header;
- remove the P-Access-Network-Info header and act upon the contents accordingly; and
- route the request based on the topmost Route header.

5.4.3.3 Requests terminated at the served user

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

1) remove its own URL from the topmost Route header;
2) check if P-Original-Dialog-ID header is present in the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The od-to-tag, od-from-tag and od-call-id parameter values from the P-Original-Dialog-ID header may be used as additional parameters when searching for existing dialogs. The S-CSCF shall determine the next hop using initial filter criteria. If the next hop is another Application Server, the S-CSCF shall retain the P-Original-Dialog-ID header in the message of the request. If the next hop is not an Application Server, the S-CSCF shall remove the P-Original-Dialog-ID header from the request;
3) check whether the initial request matches the initial filter criteria based on the public user identity in the Request-URI~~from the service profile associated with the received public user identity~~, the S-CSCF shall forward this request to that application server, then check for matching of the next following filter criteria of lower priority, and apply the filter criteria on the SIP method received from the previously contacted application server as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous process, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

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

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

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

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

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

7) in case there are no Route headers in the request, then determine, from the destination public user identity, the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2;

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

9) determine, from the destination public user identity, the saved Contact URL where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.4.3.4 Original dialog identifier

The original dialog identifier is coded as the P-Original-Dialog-ID as described in subclause 7.2.7.

5.4.3.5 Abnormal cases

The S-CSCF shall, when contacting application servers based on the initial filter criteria, expect either a final response from the application server as the session terminates there, or the initial request message, that may be modified. In either case the message should be identified (using P-Original-Dialog-ID) as belonging to the original request forwarded by the S-CSCF.

If the S-CSCF receives a message including an P-Original-Dialog-ID that does not match any that it has forwarded to the application server it shall:

- respond to the application server with 481 Call Leg/Transaction Does Not Exist.

End of second changes