3GPP TSG CN Plenary Meeting #18 **NP-020559**
4th - 6th December 2002. New Orleans, USA.

Source: **TSG CN WG 1**

Title: **CRs to Rel-5 on Work Item IMS-CCR towards 24.229,- pack 2**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **10** CRs, **Rel-5** Work Item **"IMS-CCR"**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #18 for approval.

Spec	CR #	Rev	CAT	Rel	Tdoc Title	Meeting	TDoc #	C_Version
24.229	204	3	F	Rel-5	Fix gprs-charging-info definition and descriptions	N1-27	N1-022426	5.2.0
24.229	206		F	Rel-5	Alignment of the SDP attributes related to QoS integration with IETF	N1-26	N1-021930	5.2.0
24.229	207	1	F	Rel-5	Update of the 3GPP-generated SIP P- headers document references	N1-26	N1-022116	5.2.0
24.229	208	1	F	Rel-5	Handling of INVITE requests that do not contain SDP	N1-26	N1-022098	5.2.0
24.229	209	2	F	Rel-5	UE Registration	N1-27	N1-022471	5.2.0
24.229	211	1	F	Rel-5	Usage of private user identity during registration	N1-26	N1-022083	5.2.0
24.229	212	1	F	Rel-5	P-CSCF subscription to the users registration-state event	N1-26	N1-022084	5.2.0
24.229	213	2	F	Rel-5	Handling of MT call by the P-CSCF	N1-26	N1-022154	5.2.0
24.229	215		F	Rel-5	P-CSCF acting as a UA	N1-26	N1-021939	5.2.0
24.229	216	1	F	Rel-5	S-CSCF handling of protected registrations	N1-26	N1-022085	5.2.0

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

Tdoc N1-022426

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.

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

1. IM~~S~~ CN subsystem 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 and ECF.

4.5.2 IM~~S~~ CN subsystem charging identifier (ICID)

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

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

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 IM~~S~~ CN subsystem ~~network~~ entities for one side of the session (either the calling or called side). GPRS charging information (GGSN identifier and ~~GCIDs~~PDP context information) 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 details of the gprs-charging-info parameter is described in subclause -7.2.6.~~contains further parameters: ggsn and gcidpdp-info. The gcid parameter contains charging identifiers for one or more PDP contexts, or GCID. Each gcid pdp-info parameter has an indicator if it is an IM CN subsystem signalling PDP context (pdp-sig), an GPRS charging identifier assigned by the GGSN for the PDP context (pdp-idgcid parameter), the authorizsation token used when PDP context was established (auth-token) and one or more flow identifiers an index number (pdpflow-indexflow id parameter) to correlate the PDP context with one or morea media streams 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.~~

~~When a PDP context is only used for SIP signalling, i.e. no media stream requested for a session, then there is no authorisation activity or information exchange over the Go interface. Since there are no GCID, authorisation token or flow identifiers available in this case, the gcid and auth-token parameters are set to zero and there are no flow-id parameters included.~~

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, orig-ioi, and one for the terminating side, term-ioi.

The S-CSCF in the originating network populates the 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 term-ioi parameter is left out of the P-Charging-Vector parameter. The S-CSCF in the originating network retrieves the 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 orig-ioi on behalf of the PSTN/PLMN when a call/session is originated from the PSTN/PLMN.

The S-CSCF in the terminating network retrieves the orig-ioi parameter from the P-Charging-Vector header in the initial request, which identifies the operator network from which the request originated. The S-CSCF in the terminating network populates the 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 the network, except when proxied by BGCF and I-CSCF to get to MGCF and S-CSCF. 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 IM~~S~~ CN subsystem ~~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, ccf2, ecf1 and ecf2. Only ccf1 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 an HSS via the Cx interface and passed by the S-CSCF to subsequent entities. The charging function addresses are passed from the S-CSCF to the 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) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The 'Require: sec-agree' header shall also be removed. If the header is not present, then a suitable 4xx error code shall be sent back;

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

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

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

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

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

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

1) remove and store the CK and IK values contained in the 401 (Unauthorized) response. The 401 (Unauthorized) response shall be forwarded to the UE if and only if the CK and IK have been removed;

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

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

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

1) save the list of P-Service-Route headers preserving the order. This list shall be stored during the entire registration period of the respective public user identity. This list shall be used to preload the routeing information into the initial requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of P-Service-Route headers with the new list;

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

3) remove any Path and P-Service-Route headers from the 200 (OK) response before forwarding the response to the UE;

4) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;

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

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

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

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

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

The P-CSCF shall delete any security association from the IPSec database when their SIP level lifetime expires.

End of second changes

Start of third changes

5.2.7 Initial INVITE

5.2.7.1 Introduction

In addition to following the procedures for initial requests defined in subclause 5.2.6, initial INVITE requests also follow the procedures of this subclause.

5.2.7.2 Mobile-originating case

The P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

Upon receiving a response (e.g. 183 (Session Progress), 200 (OK)) to the initial INVITE request, the P-CSCF:

- if a media authorization token is generated by the PCF as specified in RFC 3313 [31] (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

When the P-CSCF sends the UPDATE request towards the S-CSCF, the P-CSCF shall also include the ~~gprs~~access-network-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the ~~GPRS~~ access network charging information.

5.2.7.3 Mobile-terminating case

When the P-CSCF receives an initial INVITE request destined for the UE, it will contain the URL of the UE in the Request-URI, and a single pre-loaded Route header. The received initial INVITE will also have a list of Record-Route headers. Prior to forwarding the initial INVITE to the URL found in the Request-URI, the P-CSCF shall:

- if a media authorization token is generated by the PCF as specified in RFC 3313 [31] (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

In addition, the P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

When the P-CSCF sends 180 (Ringing) or 200 (OK) (to INVITE) towards the S-CSCF, the P-CSCF shall also include the ~~gprs~~access-network-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the ~~GPRS~~ access network charging information.

5.2.7.4 ~~GPRS~~ Access network charging information

The ~~GPRS access network charging information shall be coded as~~ P-CSCF shall include the ~~gprs~~access-network-charging-info parameter within the P-Charging-Vector header as described in subclause 7.2.6.

~~For the case of a GPRS access network, the access-network-charging-info parameter shall be populated with the gprs-charging-info-version of the parameter.~~

~~The gprs-charging-info parameter shall contain one ggsn child parameter and one or more child gcid pdp-info parameters. The ggsn child parameter shall contain the identifier of the associated GGSN. Each gcid pdp-info child parameter within gprs-charging- info corresponds to a PDP context that was established at the GGSN for a UE. Each gcid pdp-info parameter contains pdp-sig, gcid, pdp-id, flow-index and auth-token and flow-id child parameters. The pdp-sig parameter shall be to "yes" if the IM-CN-Subsystem-Signalling-Flag within the Protocol-Configuration-Options IE is received or "no" if the PCO IM-CN-Subsystem-Signalling-Flag is not received. The pdp-idgcid parameter shall be populated with the PDP contextGPRS charging identifier that the P-CSCF obtained from the GGSN. The auth-token and flow-id parameters shall be populated with the authorization token and one or more flow identifiers from the Traffic Flow Template IE (if available). For the case of a PDP context that is only used for SIP signalling (i.e. no media stream~~

~~requested requested for a session), the gcid and auth-token parameters shall be set to 0 and no flow-id parameters shall be included.~~The flow-index parameter shall be populated with the relative index to the media stream in the SDP for the PDP context. The auth-token parameter shall be populated with the authorization token that is associated with this PDP context for a media stream. For more information about the PDP contexts for media, see subclause 9.2.5. For the case of a PDP context that is used for signalling, the flow-index and auth-token parameters shall be set to 0.

End of third changes

Start of fourth changes

5.2.9 Subsequent requests

5.2.9.1 Mobile-originating case

For a reINVITE request from the UE, when the P-CSCF sends the UPDATE request towards the S-CSCF, the P-CSCF shall include the updated ~~gprs~~access-network-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the ~~GPRS~~ access network charging information.

5.2.9.2 Mobile-terminating case

For a reINVITE request destined towards the UE, when the P-CSCF sends 200 (OK) response (to the INVITE request) towards the S-CSCF, the P-CSCF shall include the updated ~~gprs~~access-network-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the ~~GPRS~~ access network charging information.

End of fourth changes

Start of fifth changes

5.4.4 Call initiation

5.4.4.1 Initial INVITE

Void.

5.4.4.2 Subsequent requests

5.4.4.2.1 Mobile-originating case

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

When the S-CSCF receives the 183 response, the S-CSCF shall insert a P-Charging-Function-Addresses header (see subclause 7.2.5) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

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

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

5.4.4.2.2 Mobile-terminating case

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

When the S-CSCF receives the 183 response, the S-CSCF shall insert a P-Charging-Function-Addresses header (see subclause 7.2.5) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

When the S-CSCF receives 180 (Ringing) or 200 (OK) (to INVITE) responses, the S-CSCF shall store the access-network~~gprs~~-charging-info parameter from the P-Charging-Vector header. The access-network~~gprs~~-charging-info parameter shall be retained in the P-Charging-Vector header when the response is forwarded to an AS. However, the access-network~~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 fifth changes

Start of sixth changes

5.4.6 Call-related requests

5.4.6.1 ReINVITE

5.4.6.1.1 Determination of served user

Void.

5.4.6.1.2 Mobile-originating case

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

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

5.4.6.1.3 Mobile-terminating case

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

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

End of sixth changes

Start of seventh changes

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. See 3GPP TS 32.225 [17] for requirements on the format of ICID.
- Inter Operator Identifier (IOI), which are globally unique identifiers for a particular network.
- Access Network Charging Information, which is charging information specific to the type of access network. ~~where the GPRS is the initially supported access network. For GPRS there are the following components to track: GGSN address and one or more PDP contexts. Each PDP context has an indicator if it is an IM CN subsystem signalling PDP context, an associated GPRS Charging Identifiers (GCID), an authorisation token and one or more flow identifiers that identify associated m-lines within the SDP from the SIP signalling. For a PDP context that is only used for SIP signalling, i.e. no media stream requested requested for a session, then there is no authorisation activity or information exchange over the Go interface. Since there are no GCID, authorisation token or flow identifiers in this case, the GCID and authorisation token are set to zero and no flow identifier parameters are included. 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 draft-garcia-sipping-3gpp-p-headers ~~table 7.3, which is extracted from draft-henrikson-sip-charging-information~~ [~~45~~5244]. 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-valuegeneric-param)
gprs-charging-info = "gprs-charging-info" SEMI
                     "ggsn" EQUAL ggsn *(SEMI pdp-info"gcid" EQUAL gcid)
                     [COMMA SEMI extension-param]
ggsn = "ggsn" EQUAL gen-value
pdp-info = pdp-sig SEMI gcid SEMI auth-token *(SEMI flow-id)
pdp-sig = "pdp-sig" EQUAL ("yes" / "no")
gcid = "pdp-idgcid" EQUAL gen-valuepdp-id COMMA "flow-index" EQUAL flow-index
       COMMA "auth-token" EQUAL auth-token
pdp-id = gen-value
flow-index = gen-value
auth-token = "auth-token" EQUAL gen-value
flow-id = "flow-id" EQUAL gen-value
extension-param = token [EQUAL (token | quoted-string)]
```

The access-network-charging-info parameter is an instance of generic-param from the current charge-params component of P-Charging-Vector header

The access-network-charging-info parameter includes alternative definitions for different types access networks.

GPRS is the initially supported access network (gprs-charging-info parameter). For GPRS there are the following components to track: GGSN address (ggsn parameter) and one or more PDP contexts (pdp-info parameter). Each PDP

context has an indicator if it is an IM CN subsystem signalling PDP context (pdp-sig parameter), an associated GPRS Charging Identifier (gcid parameter), a media ~~n~~ authorizsation token (auth-token parameter) and one or more flow identifiers (flow-id parameter) that identify associated m-lines within the SDP from the SIP signalling. These parameters are transferred from the GGSN to the P-CSCF (PDF) over the Go interface, see 3GPP TS 29.207[12].~~See 3GPP TS 29.207 [12] for the requirements on the format of the data received over the Go interface that is populated into the pdp-info child parameter of gprs-charging-info.~~

For a PDP context that is only used for SIP signalling, i.e. no media stream requested requested for a session, then there is no authorisation activity or information exchange over the Go interface. Since there are no GCID, media authorizsation token or flow identifiers in this case, the GCID and media authorizsation token are set to zero and no flow identifier parameters are constructed by the P-CSCF~~included~~.

~~The gprs-charging-info parameter contains one ggsn-child parameter and one or more child gcid pdp-info parameters. For further information, see clause 5.2.7.4.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 seventh changes

3GPP TSG-CN1 Meeting #26
Miami Beach, Florida, USA, 23 – 27 September 2002

Tdoc N1-021930

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **206** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

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

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

Title:	⌘	Alignment of the SDP attributes related to QoS integration with IETF
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	12/09/2002
Category:	⌘	**F**
Release:	⌘	Rel-F

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 Annex A.3 defines the SDP profile. The tables still refers to an old syntax of RFC 3312, when it was an internet draft
Summary of change:	⌘	• Modification of tables A.319 and A.330 in Annex A.3: the "a=qos" SDP attribute is replaced by "a=curr", "a=des" and "a=conf" • Editorial error fixed: There is a duplication of subclause A.3.2.3. The second appearance of A.3.2.3 is renamed to A.3.3.3, as it is part of subclause A.3.3.
Consequences if not approved:	⌘	Incompatible semantics definition with RFC 3312

Clauses affected:	⌘	A.3				
Other specs affected:	⌘	**Y**	**N**		⌘	
		X		Other core specifications		24.228
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

A.3 Profile definition for the Session Description Protocol as used in the present document

A.3.1 Introduction

Void.

A.3.2 User agent role

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for UA implementations.

Prerequisite: A.2/1 -- user agent role

A.3.2.1 Major capabilities

Table A.317: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
	Extensions			
22	Integration of resource management and SIP?	[30]	o	m

A.3.2.2 SDP types

Table A.318: SDP types

Item	Type	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
	Session level description						
1	v= (protocol version)	[39] 6	m	m	[39] 6	m	m
2	o= (owner/creator and session identifier)	[39] 6	m	m	[39] 6	m	m
3	s= (session name)	[39] 6	m	m	[39] 6	m	m
4	i= (session information)	[39] 6	o		[39] 6		
5	u= (URI of description)	[39] 6	o	n/a	[39] 6		n/a
6	e= (email address)	[39] 6	o	n/a	[39] 6		n/a
7	p= (phone number)	[39] 6	o	n/a	[39] 6		n/a
8	c= (connection information)	[39] 6	o		[39] 6		
9	b= (bandwidth information)	[39] 6	o	o (NOTE 1)	[39] 6		
	Time description (one or more per description)						
10	t= (time the session is active)	[39] 6	m	m	[39] 6	m	m
11	r= (zero or more repeat times)	[39] 6	o	n/a	[39] 6		n/a
	Session level description (continued)						
12	z= (time zone adjustments)	[39] 6	o	n/a	[39] 6		n/a
13	k= (encryption key)	[39] 6	o		[39] 6		
14	a= (zero or more session attribute lines)	[39] 6	o		[39] 6		
	Media description (zero or more per description)						
15	m= (media name and transport address)	[39] 6	o	o	[39] 6	m	m
16	i= (media title)	[39] 6	o		[39] 6		
17	c= (connection information)	[39] 6	c1	c1	[39] 6		
18	b= (bandwidth information)	[39] 6	o	o (NOTE 1)	[39] 6		
19	k= (encryption key)	[39] 6	o		[39] 6		
20	a= (zero or more media attribute lines)	[39] 6	o		[39] 6		
c1: IF A.318/15 THEN m ELSE n/a.							
NOTE 1: For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified.							

Prerequisite A.318/14 OR A.318/20 - - a= (zero or more session/media attribute lines)

Table A.319: zero or more session / media attribute lines (a=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	category (a=cat)	[39] 6			[39] 6		
2	keywords (a=keywds)	[39] 6			[39] 6		
3	name and version of tool (a=tool)	[39] 6			[39] 6		
4	packet time (a=ptime)	[39] 6			[39] 6		
5	maximum packet time (a=maxptime)	[39] 6			[39] 6		
6	receive-only mode (a=recvonly)	[39] 6			[39] 6		
7	send and receive mode (a=sendrecv)	[39] 6			[39] 6		
8	send-only mode (a=sendonly)	[39] 6			[39] 6		
9	whiteboard orientation (a=orient)	[39] 6			[39] 6		
10	conference type (a=type)	[39] 6			[39] 6		
11	character set (a=charset)	[39] 6			[39] 6		
12	language tag (a=sdplang)	[39] 6			[39] 6		
13	language tag (a=lang)	[39] 6			[39] 6		
14	frame rate (a=framerate)	[39] 6			[39] 6		
15	quality (a=quality)	[39] 6			[39] 6		
16	format specific parameters (a=fmtp)	[39] 6			[39] 6		
17	rtpmap attribute (a=rtpmap)	[39] 6			[39] 6		
~~18~~	~~qos-attribute (a=qos)~~	~~[30] 5~~	~~c1~~	~~c1~~	~~[30] 5~~	~~c2~~	~~c2~~
18	current-status attribute (a=curr)	[30] 5	c1	c1	[30] 5	c2	c2
19	desired-status attribute (a=des)	[30] 5	c1	c1	[30] 5	c2	c2
20	confirm-status attribute (a=conf)	[30] 5	c1	c1	[30] 5	c2	c2
c1:	IF A.317/22 THEN o ELSE n/a.						
c2:	IF A.317/22 THEN m ELSE n/a.						

A.3.2.3 SDP types parameters

Prerequisite A.318/2 - - o= (owner/creator and session identifier)

Table A.320: owner/creator and session identifier type (o=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	username	[39] 6	m	m	[39] 6	m	n/a
2	session id	[39] 6	m	m	[39] 6	m	m
3	version	[39] 6	m	m	[39] 6	m	m
4	network type	[39] 6	m	m	[39] 6	m	n/a
5	address type	[39] 6	m	m	[39] 6	m	n/a
6	address	[39] 6	m	m	[39] 6	m	n/a

Prerequisite A.318/10 - - t= (time the session is active)

Table A.321: time the session is active type (t=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	start time	[39] 6	m	m	[39] 6	m	n/a
2	stop time	[39] 6	m	m	[39] 6	m	n/a

Prerequisite A.318/11 - - r= (zero or more repeat times)

Table A.322: zero or more repeat times (r=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	repeat interval	[39] 6		n/a	[39] 6		n/a
2	active duration	[39] 6		n/a	[39] 6		n/a
3	list of offsets from start-time	[39] 6		n/a	[39] 6		n/a

Prerquisite A.318/12 - - z= (time zone adjustments)

Table A.323: time zone adjustments type (z=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	adjustment time	[39] 6		n/a	[39] 6		n/a
2	offset	[39] 6		n/a	[39] 6		n/a
3	adjustment time	[39] 6		n/a	[39] 6		n/a
4	offset	[39] 6		n/a	[39] 6		n/a

Prerquisite A.318/13 - - k= (encryption key)

Table A.324: encryption key type (k=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	method	[39] 6			[39] 6		
2	encryption key	[39] 6			[39] 6		

Prerequisite A.318/15 - - m= (media name and transport address)

Table A.325: media name and transport address type (m=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	media - ``audio'' - ``video'' - ``application'' - ``data'' - ``control''	[39] 6			[39] 6		
2	port	[39] 6			[39] 6		
3	transport	[39] 6			[39] 6		
4	fmt list	[39] 6			[39] 6		

Editor's note: It is expected that this table will be expanded, as this is the principle table that will distinguish operation of different entities within the IM CN subsystem.

Prerequisite A.318/17 - - c= (connection information)

Table A.326: connection type (c=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	network type	[39] 6			[39] 6		
2	address type	[39] 6			[39] 6		
3	connection address	[39] 6			[39] 6		

Prerequisite A.318/18 - - b= (bandwidth information)

Table A.327: bandwidth information (b=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	modifier	[39] 6		o (NOTE 1)	[39] 6		
2	bandwidth-value	[39] 6		o (NOTE 2)	[39] 6		
NOTE 1: For "video" and "audio" media types that utilise RTP/RTCP, the value shall be AS. NOTE 2: For "video" and "audio" media types that utilise RTP/RTCP, it shall be specified. For other media types, it may be specified.							

A.3.3 Proxy role

This subclause contains the ICS proforma tables related to the user role. They need to be completed only for proxy implementations.

Prerequisite: A.2/2 -- proxy role

A.3.3.1 Major capabilities

Table A.328: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
	Extensions			
1	Integration of resource management and SIP?	[30]	o	m

A.3.3.2 SDP types

Table A.329: SDP types

Item	Type	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
	Session level description						
1	v= (protocol version)	[39] 6	m	m	[39] 6	m	m
2	o= (owner/creator and session identifier).	[39] 6	m	m	[39] 6	i	i
3	s= (session name)	[39] 6	m	m	[39] 6	i	i
4	i= (session information)	[39] 6	m	m	[39] 6	i	i
5	u= (URI of description)	[39] 6	m	m	[39] 6	i	i
6	e= (email address)	[39] 6	m	m	[39] 6	i	i
7	p= (phone number)	[39] 6	m	m	[39] 6	i	i
8	c= (connection information)	[39] 6	m	m	[39] 6	i	i
9	b= (bandwidth information)	[39] 6	m	m	[39] 6	i	i
	Time description (one or more per description)						
10	t= (time the session is active)	[39] 6	m	m	[39] 6	i	i
11	r= (zero or more repeat times)	[39] 6	m	m	[39] 6	i	i
	Session level description (continued)						
12	z= (time zone adjustments)	[39] 6	m	m	[39] 6	i	i
13	k= (encryption key)	[39] 6	m	m	[39] 6	i	i
14	a= (zero or more session attribute lines)	[39] 6	m	m	[39] 6	i	i
	Media description (zero or more per description)						
15	m= (media name and transport address)	[39] 6	m	m	[39] 6	m	m
16	i= (media title)	[39] 6	o		[39] 6		
17	c= (connection information)	[39] 6	o		[39] 6		
18	b= (bandwidth information)	[39] 6	o		[39] 6		
19	k= (encryption key)	[39] 6	o		[39] 6		
20	a= (zero or more media attribute lines)	[39] 6	o		[39] 6		

Prerequisite A.329/14 OR A.329/20 - - a= (zero or more session/media attribute lines)

Table A.330: zero or more session / media attribute lines (a=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	category (a=cat)	[39] 6			[39] 6		
2	keywords (a=keywds)	[39] 6			[39] 6		
3	name and version of tool (a=tool)	[39] 6			[39] 6		
4	packet time (a=ptime)	[39] 6			[39] 6		
5	maximum packet time (a=maxptime)	[39] 6			[39] 6		
6	receive-only mode (a=recvonly)	[39] 6			[39] 6		
7	send and receive mode (a=sendrecv)	[39] 6			[39] 6		
8	send-only mode (a=sendonly)	[39] 6			[39] 6		
9	whiteboard orientation (a=orient)	[39] 6			[39] 6		
10	conference type (a=type)	[39] 6			[39] 6		
11	character set (a=charset)	[39] 6			[39] 6		
12	language tag (a=sdplang)	[39] 6			[39] 6		
13	language tag (a=lang)	[39] 6			[39] 6		
14	frame rate (a=framerate)	[39] 6			[39] 6		
15	quality (a=quality)	[39] 6			[39] 6		
16	format specific parameters (a=fmtp)	[39] 6			[39] 6		
17	rtpmap attribute (a=rtpmap)	[39] 6			[39] 6		
~~18~~	~~qos-attribute (a=qos)~~	~~[30] 5~~	~~m~~	~~m~~	~~[30] 5~~	~~c2~~	~~c2~~
18	current-status attribute (a=curr)	[30] 5	m	m	[30] 5	c2	c2
19	desired-status attribute (a=des)	[30] 5	m	m	[30] 5	c2	c2
20	confirm-status attribute (a=conf)	[30] 5	m	m	[30] 5	c2	c2
c2:	IF A.328/1 THEN m ELSE i.						

A.3.32.3 SDP types parameters

Prerequisite A.329/2 - - o= (owner/creator and session identifier)

Table A.331: owner/creator and session identifier type (o=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	username	[39] 6	m	m	[39] 6	m	m
2	session id	[39] 6	m	m	[39] 6	m	m
3	version	[39] 6	m	m	[39] 6	m	m
4	network type	[39] 6	m	m	[39] 6	m	m
5	address type	[39] 6	m	m	[39] 6	m	m
6	address	[39] 6	m	m	[39] 6	m	m

Prerequisite A.329/10 - - t= (time the session is active)

Table A.332: time the session is active type (b=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	start time	[39] 6			[39] 6		
2	stop time	[39] 6			[39] 6		

Prerequisite A.329/11 - - r= (zero or more repeat times)

Table A.333: zero or more repeat times (r=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	repeat interval	[39] 6			[39] 6		
2	active duration	[39] 6			[39] 6		
3	list of offsets from start-time	[39] 6			[39] 6		

Prerequisite A.329/12 - - z= (time zone adjustments)

Table A.334: time zone adjustments type (z=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	adjustment time	[39] 6			[39] 6		
2	offset	[39] 6			[39] 6		
3	adjustment time	[39] 6			[39] 6		
4	offset	[39] 6			[39] 6		

Prerequisite A.329/13 - - k= (encryption key)

Table A.335: encryption key type (k=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	method	[39] 6			[39] 6		
2	encryption key	[39] 6			[39] 6		

Prerequisite A.329/15 - - m= (media name and transport address)

Table A.336: media name and transport address type (m=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	media - ``audio'' - ``video'' - ``application'' - ``data'' - ``control''	[39] 6			[39] 6		
2	port	[39] 6			[39] 6		
3	transport	[39] 6			[39] 6		
4	fmt list	[39] 6			[39] 6		

Editor's note: It is expected that this table will be expanded, as this is the principle table that will distinguish operation of different entities within the IM CN subsystem.

Prerequisite A.329/17 - - c= (connection information)

Table A.337: connection type (c=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	network type	[39] 6			[39] 6		
2	address type	[39] 6			[39] 6		
3	connection address	[39] 6			[39] 6		

Prerequisite A.329/18 - - b= (bandwidth information)

Table A.338: bandwidth information (b=)

Item	Field	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	modifier	[39] 6			[39] 6		
2	bandwidth-value	[39] 6			[39] 6		

3GPP TSG-CN1 Meeting #26
Miami Beach, Florida, USA, 23 – 27 September 2002

Tdoc N1-022116

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **207** ⌘ **rev** **1** ⌘ Current version: **5.2.0** ⌘

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

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

Title:	⌘	Update of the 3GPP-generated SIP P- headers document references
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	25/09/2002
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 3GPP-generated SIP P- headers were originally specified in independent documents. However, all these documents have been merged into a single Internet Draft that defines all the 3GPP-generated SIP P- headers
Summary of change:	⌘	• Make void old individual Internet drafts from the clause 2. • Added a new reference with the current merged Internet Draft. • Fixed text in section 7 that points to the individual drafts, so that it now points to the current merged Internet Draft • The syntax of the P-Called-Party-ID header is replaced by a pointer to the IETF specification. • Added a new subclause 7.2.10 for the P-Assciated-URI header
Consequences if not approved:	⌘	References to old documents that will not progress towards RFC.

Clauses affected:	⌘	2, 7

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

Other comments:	⌘	

First proposed change

2 References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[24] RFC 2916 (June 1999): "E.164 number and DNS".

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

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

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

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

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

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

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

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

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

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

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

[36] draft-ietf-sip-refer-05 (June 2002): "The REFER method".

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

[37] draft-sparks-sip-mimetypes-03 (April 2002): "Internet Media Type message/sipfrag".

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

[38] draft-willis-scvrtdisco-06 (May 2002): "SIP Extension Header for Service Route Discovery in Private Networks".

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

[39] draft-ietf-mmusic-sdp-new-10 (May 2002): "SDP: Session Description Protocol".

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

[40] draft-ietf-dhc-dhcpv6-26 (June 2002): "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

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

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

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

[42] draft-ietf-sipping-sigcomp-sip-dictionary-03.txt (July 2002): "The SIP/SDP static dictionary for Signaling Compression".

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

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

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

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

~~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".~~void

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

[46] Void.

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

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

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

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

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

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

[50] draft-ietf-sip-message-06.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.

[51] 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.

[52] draft-garcia-sipping-3gpp-p-headers-01.txt (August 2002): "Private Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)".

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

Next proposed change

7 Extensions within the present document

7.1 SIP methods defined within the present document

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

7.2 SIP headers defined within the present document

7.2.1 Void

7.2.2 P-Called-Party-ID header

7.2.2.1 Introduction

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

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

7.2.2.2 Syntax

The syntax of the P-Called-Party-ID header is described in draft-garcia-sipping-3gpp-p-headers [52]~~The P-Called-Party-ID header field has the syntax described in table 7.1.~~

~~Table 7.1: Syntax of P-Called-Party-ID header~~

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

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

~~Table 7.2 is an extension of tables 2 and 3 in RFC 3261 [26] and table in subclause 7.5 in RFC 3265 [28].~~

~~Table 7.2: P-Called-Party-ID header~~

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

7.2.2.3 Operation

The operation of this header is described in subclause 5.4.3.3.

7.2.3 P-Access-Network-Info header

7.2.3.1 Introduction

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

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

The S-CSCF shall remove the P-Access-Network-Info header from any message where it is present, before it forwards the message. The S-CSCS shall act accordingly upon the information received in the P-Access-Network-Info header.

7.2.3.2 Syntax

The syntax of the P-Access-Network-Info header is described in draft-garcia-sipping-3gpp-p-headers [52]~~draft-mills-sip-access-network-info-02.txt [47]~~.

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

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

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

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

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

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

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

7.2.4 P-Visited-Network-ID header

7.2.4.1 Introduction

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

7.2.4.2 Syntax

The P-Visited-Network-ID header field has the syntax described in draft-garcia-sipping-3gpp-p-headers [52]~~draft-garcia-sip-visited-network-id [44]~~.

7.2.4.3 Operation

The header is inserted by the P-CSCF in every REGISTER request the UE sends. The I-CSCF sends the contents of the header to the HSS. Additional details are provided in subclause 5.2.2

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 (ccf1) address is a required parameter for offline charging. The secondary CCF address is optional (ccf2). Both the primary and secondary Event Charging Function (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-garcia-sipping-3gpp-p-headers [52] ~~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. See 3GPP TS 32.225 [17] for requirements on the format of ICID.
- 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 draft-garcia-sipping-3gpp-p-headers [52].~~in table 7.3, which is extracted from draft-henrikson-sip-charging-information [45]~~. Table 7.3 describes extensions required for 3GPP to that syntax.

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.

7.2.7 Void

7.2.8 P-Service-Route header

The P-Service-Route header is defined in draft-willis-scvrtdisco [38].

7.2.9 P-Asserted-Identity header

7.2.9.1 Introduction

The P-Asserted-Identity header is the mechanism whereby the first element in the trust domain (see subclause 4.4) may assert a public user identity identifying the user. The P-Asserted-Identity header can also be used as a hint to the first element in the trust domain when it selects the asserted public user identity.

The header is inserted at the first opportunity when initialising dialogs and with standalone transactions. The header may be included in requests and responses.

7.2.9.2 Syntax

The P-Asserted-Identity header field has the syntax described in RFC 3325 [34].

7.2.9.3 Operation

The operation of this header is described in clause 5.

7.2.10 P-Associated-URI header

7.2.10.1 Introduction

The P-Associated-URI header is used to allow the home network (e.g, the S-CSCF) to return a set of associated URIs with the public user identity under registration. This header is only used in the 200 (OK) response for a REGISTER request.

7.2.10.2 Syntax

The P-Associated-URI header field has the syntax described in draft-garcia-sipping-3gpp-p-headers [52].

7.2.10.3 Operation

The header is inserted by the S-CSCF in every 200 (OK) response for a REGISTER request. Additional information is provided in subclauses 5.1.1.2, 5.1.1.4, 5.2.2 and 5.4.1.2.2

7.2A Extensions to SIP headers defined within the present document

7.2A.1 Extension to WWW-authenticate header

7.2A.1.1 Introduction

This extension defines a new authentication parameter (auth-param) for the WWW-Authenticate header used in a 401 (Unauthorized) response to the REGISTER request. For more information, see RFC 2617 [21] subclause 3.2.1.

7.2A.1.2 Syntax

The syntax for for auth-param is specified in table 7.4.

Table 7.4: Syntax of auth-param

```
auth-param      = 1#( integrity-key / cipher-key )
integrity-key   = "ik" EQUAL ik-value
cipher-key      = "ck" EQUAL ck-value
ik-value        = LDQUOT *(HEXDIG) RDQUOT
ck-value        = LDQUOT *(HEXDIG) RDQUOT
```

7.2A.1.3 Operation

This authentication parameter will be used in a 401 (Unauthorized) response in the WWW-authenticate header during UE authentication procedure as specified in subclause 5.4.1.

The S-CSCF appends the integrity-key parameter (directive) to the WWW.-Authenticate header in a 401 (Unauthorized) response. The P-CSCF stores the integrity-key value and removes the integrity-key parameter from the header prior to forwarding the response to the UE.

The S-CSCF appends the cipher-key parameter (directive) to the WWW-Authenticate header in a 401 (Unauthorized) response. The P-CSCF removes the cipher-key parameter from the header prior to forwarding the response to the UE. In the case ciphering is used, the P-CSCF stores the cipher-key value.

7.2A.2 integrity-protected parameter (directive)

7.2A.2.1 Introduction

The integrity-protected authentication parameter (auth-param) is an extension parameter defined for the Authorization header used in REGISTER requests. For more information, see RFC 2617 [21] subclause 3.2.2.

7.2A.2.2 Syntax

The syntax for for auth-param is specified in table 7.5.

Table 7.5: Syntax of auth-param

```
integrity-protected = “integrity-protected” EQUAL (“yes” / “no”)
```

7.2A.2.3 Operation

This authentication parameter is inserted by the P-CSCF in all the REGISTER requests received from the UE. The value of the parameter is set to “yes” in case the request was integrity protected, otherwise the value of it is set to “no”. This information is used by S-CSCF to decide whether to challenge the REGISTER request or not, as specified in subclause 5.4.1.

7.2A.3 Tokenized-by parameter definition

7.2A.3.1 Introduction

The tokenized-by parameter is an extension parameter appended to encrypted entries in various SIP headers as defined in subclause 5.3.3.1.

7.2A.3.2 Syntax

The syntax for the tokenized-by parameter is specified in table 7.6:

Table 7.6: Syntax of tokenized-by-param

```
uri-parameter =  transport-param / user-param / method-param
/ ttl-param / maddr-param / lr-param / tokenized-by-param / other-param
tokenized-by-param = “tokenized-by” EQUAL hostname
```

The BNF for uri-parameter is taken from IETF RFC 3261 [26] and modified accordingly.

7.2A.3.3 Operation

The tokenized-by parameter is appended by I-CSCF(THIG) after all encrypted strings within SIP headers when network configuration hiding is active. The value of the parameter is the domain name of the network which encrypts the information.

7.3 Option-tags defined within the present document

There are no option-tags defined within the present document over and above those defined in the referenced IETF specifications.

7.4 Status-codes defined within the present document

There are no status-codes defined within the present document over and above those defined in the referenced IETF specifications.

7.5 Session description types defined within the present document

There are no session description types defined within the present document over and above those defined in the referenced IETF specifications.

7.6 3GPP IM CN subsystem XML body, version 1

7.6.1 General

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

Any SIP User Agent or proxy may insert or remove the 3GPP IM CN subsystem XML body or parts of it, as required, in any SIP message. The 3GPP IM CN subsystem XML body shall not be forwarded outside a 3GPP network.

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

7.6.2 Document Type Definition

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

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

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

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

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

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

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

]>
```

7.6.3 DTD description

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

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

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

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

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

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

7.7 SIP timers

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

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

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

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

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

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

Table 7.8: SIP timers

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

3GPP TSG-CN1 Meeting #26
Miami Beach, Florida, USA, 23 – 27 September 2002

Tdoc N1-022098

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **208** ⌘ **rev** **1** ⌘ Current version: **5.2.0** ⌘

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

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

Title:	⌘	Handling of INVITE requests that do not contain SDP
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	25/09/2002
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 current specification assumes that all the INVITE requests sent or received by the UE will contain SDP. While that is the common case, and the forced case to mobile originated INVITEs, it may be possible than an Applicacion Server or any other entity acting as a third party call controller will send an INVITE that do not contain SDP. Handling of this INVITEs is not specified in the specification. The issue affects also the generation of the inclusion of the P-Media-Authorization token in the SIP message. At the moment, the inclusion is dependent on the SIP message, rather than the presence of SDP sent to the UE that contains SDP with one or more m lines.
Summary of change:	⌘	• Clarified that the P-Media-Authorization is generated independently of the presence of absence of SDP in the SIP request or response • Clarified in the SDP procedures that the UE can receive an INVITE that does not contain SDP or the SDP does not include any "m=" media descriptions • Clarified in the SDP procedures tha the P-CSCF and S-CSCF may receive SIP INVITEs without SDP.
Consequences if not approved:	⌘	Unspecified procedures for cases where the INVITE does not contain SDP, or the SDP does not include any m lines.

Clauses affected:	⌘	5.2.7, 6

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

Other comments: ⌘

First proposed change

5.2.7 Initial INVITE

5.2.7.1 Introduction

In addition to following the procedures for initial requests defined in subclause 5.2.6, initial INVITE requests also follow the procedures of this subclause.

5.2.7.2 Mobile-originating case

The P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

Upon receiving a response (e.g. 183 (Session Progress), 200 (OK)) to the initial INVITE request, the P-CSCF:

- if a media authorization token is generated by the PCF as specified in RFC 3313 [31] (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

NOTE: Typically, the first 183 (Session Progress) response contains an SDP answer including one or more "m=" media descriptions, but it is also possible that the response does not contain an SDP answer or the SDP does not include at least an "m=" media description. However, the media authorization token is generated independently of the presence of absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value.

When the P-CSCF sends the UPDATE request towards the S-CSCF, the P-CSCF shall also include the gprs-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the GPRS charging information.

5.2.7.3 Mobile-terminating case

When the P-CSCF receives an initial INVITE request destined for the UE, it will contain the URL of the UE in the Request-URI, and a single pre-loaded Route header. The received initial INVITE request will also have a list of Record-Route headers. Prior to forwarding the initial INVITE to the URL found in the Request-URI, the P-CSCF shall:

- if a media authorization token is generated by the PCF as specified in RFC 3313 [31] (i.e. when service-based local policy control is applied), insert the P-Media-Authorization header containing that media authorization token.

NOTE: Typically, the initial INVITE request contains an SDP offer including one or more "m=" media descriptions, but it is also possible that the INVITE request does not contain an SDP offer or the SDP does not include at least an "m= media description. However, the media authorization token is generated independently of the presence of absence of "m=" media descriptions and sent to the UE in the P-Media-Authorization header value.

In a ddition, the P-CSCF shall respond to all INVITE requests with a 100 (Trying) provisional response.

When the P-CSCF sends 180 (Ringing) or 200 (OK) (to INVITE) towards the S-CSCF, the P-CSCF shall also include the gprs-charging-info parameter in the P-Charging-Vector header. See subclause 5.2.7.4 for further information on the GPRS charging information.

5.2.7.4 GPRS charging identifier

The GPRS charging information shall be coded as the gprs-charging-info parameter within the P-Charging-Vector header as described in subclause 7.2.6.

The gprs-charging-info parameter shall contain 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 shall be populated with the PDP context identifier that the P-CSCF obtained from the GGSN. The flow-index parameter shall be populated with the relative index to the media stream in the SDP for the PDP context. The auth-token parameter shall be populated with the authorization token that is associated with this PDP context for a media stream. For more information about the PDP contexts for media, see subclause 9.2.5. For the case of a PDP context that is used for signalling, the flow-index and auth-token parameters shall be set to 0.

Next proposed change

6 Application usage of SDP

6.1 Procedures at the UE

Usage of SDP by the UE:

1. In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect and possibly modify the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

2. An INVITE request generated by a UE shall contain SDP payload. The SDP payload shall reflect the calling user's terminal capabilities and user preferences for the session. In addition, the calling user shall indicate the desired QoS for the session, using the segmented status type. In an initial INVITE request the UE shall indicate that it mandates local QoS and that this precondition is not yet satisfied, i.e. the UE shall include the following preconditions:

   a=des: qos mandatory local sendrecv

   a=curr: qos local none

3. Providing that the INVITE request received by the UE contains an SDP offer including one or more "m=" media descriptions, ~~T~~the first 183 (Session Progress) provisional response ~~sent out~~ that the UE sends, shall contain the answer for the SDP received in the INVITE. The said SDP ~~payload~~ answer shall reflect the called user's terminal capabilities and user preferences.

4. When the UE sends ~~out a~~~~n~~ 183 (Session Progress) response with SDP payload including one or more "m=" media descriptions, it shall request confirmation for the result of the resource reservation at the originating end point.

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

6. For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor in the SDP. For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208 [13].

7. The UE shall include the DTMF media format at the end of the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 2833 [23].

6.2 Procedures at the P-CSCF

When the P-CSCF receives ~~an INVITE request or reINVITE request~~any SIP request or response containing SDP, the P-CSCF shall examine the media parameters in the received SDP, and remove those which are not allowed on the network by local policy. The P-CSCF will also remove those codecs from the approved media streams which are not allowed by local policy. If the P-CSCF modifies the SDP, it shall also revise the SDP to reflect the modified bandwidth requirements. For the rejected media streams, the P-CSCF should ignore the b= lines.

6.3 Procedures at the S-CSCF

When the S-CSCF receives ~~an INVITE request or reINVITE request,~~any SIP request or response containing SDP the S-CSCF shall examine the media parameters in the received SDP, and remove those media streams which are not allowed based on the subscription. The S-CSCF will also remove those codecs from the approved media streams which are not allowed by the subscription. If the S-CSCF modifies the SDP, it shall also revise the SDP to reflect the modified bandwidth requirements. For the rejected media streams, the S-CSCF should ignore the b= lines.

6.4 Procedures at the MGCF

The usage of SDP by the MGCF is the same as its usage by the UE, as defined in the subclause 6.1 and A.3.2. When sending an SDP, the MGCF shall not include the "i", "u", "e", "p", "r", and "z" descriptors in the SDP, and it shall ignore them when received in the SDP.

6.4.1 Calls originating from circuit-switched networks

When the MGCF generates and sends an INVITE request for a call originating in a circuit-switched network, the MGCF shall:

- populate the SDP with the codecs supported by the associated MGW (see 3GPP TS 26.235 [10] for the supported codecs).

When the MGCF receives 183 (Session Progress) response to an INVITE request, the MGCF shall:

- check that a supported codec has been indicated in the SDP.

6.4.2 Calls terminating in circuit-switched networks

When the MGCF receives an initial INVITE request, the MGCF shall:

- check for a codec that matches the requested SDP, which may include DTMF support.

When the MGCF generates and sends a 183 (Session Progress) response to an initial INVITE request, the MGCF shall:

- set SDP indicating the selected codec, which may include DTMF support.

6.5 Procedures at the MRFC

Void.

3GPP TSG-CN1 Meeting #27 **Tdoc N1-022471**
Bangkok, Thailand,11 – 15 November 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **209** ⌘ **rev** **2** ⌘ Current version: **5.2.0** ⌘

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

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

Title:	⌘	UE Registration
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	15/11/2002
Category:	⌘	**F**
Release:	⌘	*Rel-5*

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

Use one of the following releases:

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

Reason for change:	⌘	Collision with another CR.~~Improper use of terminology, and incomplet information in the Note.~~
Summary of change:	⌘	One (Unauthorized) addition has been removed.~~Proper use of terminology and additional text in the Note indicating that there is an alternatwe method of discovering implicitly registered public user identities.~~
Consequences if not approved:	⌘	Problems implementing the CRs.~~Reader may misunderstand the specification.~~

Clauses affected:	⌘	5.1.1.2, 5.1.1.4, 5.1.1.6, and 5.1.2.1

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

⌘

Other comments:	⌘	Revision 1 corrects the text in subclause 5.1.1.2 pertraining to IK, indicating that it is derived and not received. The text in subclause is not modified, since the same text is modified in CR N1-022034.

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

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

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

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

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

5.1.1.2 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~~ derived as a result of ~~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 username ~~ID~~ field ~~of the authentication protocol, carried~~ in the Authorization header, shall contain the private user identity;

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

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

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

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

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

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

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

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

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

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

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

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

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

5.1.1.4 User-initiated re-registration

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

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

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

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

a) the username ~~ID~~ field ~~of the authentication protocol, carried~~ in the Authorization header, shall contain the private user identity. This shall be extracted from the USIM;

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

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

d) the Expires header, or the expires parameter within the Contact header, should contain the same expiration timer as the expiration timer returned in the 200 (OK) response to the initial REGISTER request; ~~and~~

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

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

NOTE 1: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

NOTE 2: The security setup mechanism is not used in the way described in draft-ietf-sip-sec-agree [48]. The 401(Unauthorized) challenge sent back by the S-CSCF to the UE as a response to the REGISTER request is piggybacked by the P-CSCF to insert the Security-Server header field in it. The S-CSCF authenticates the UE, while the P-CSCF negotiates and sets up the security association with the UE during the same registration procedure.

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

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

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

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

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

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

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

5.1.1.6 Mobile-initiated deregistration

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

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

a) the username ~~ID~~ field ~~of the authentication protocol, carried~~ in the Authorization header, shall contain the private user identity. This shall be extracted from the USIM;

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

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

d) the Expires header, or the expires parameter of the Contact header, shall contain a value of zero, appropriate to the deregistration requirements of the user~~.~~; and

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

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

The request shall be sent integrity protected.

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

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 reg event package the UE shall perform the following actions:

- if a state parameter "active", 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 state parameter "terminated", 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 different mechanism (to the 200 (OK) response to the REGISTER request) to inform the UE about these automatically registered public user identities.

3GPP TSG-CN1 Meeting #26 ***Tdoc N1-022083***
Miami Beach, Florida, USA, 23 – 27 September 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **211** ⌘ **rev** **1** ⌘ Current version: **5.2.0** ⌘

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

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

Title:	⌘	Usage of private user identity during registration
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	15/09/2002
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:	⌘	To insure that authenticated user registers its own public user identity~~,~~ or de-registers its own public user identity.
Summary of change:	⌘	Additional text indicating that the integrity-protected REGISTER request contains the authorized private user identity.
Consequences if not approved:	⌘	Incomplete specification.

Clauses affected:	⌘	5.2.2			
		Y	**N**		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	Revision 1 incorporates the modifications requested by the working group.			

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

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

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

5.2.2 Registration

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

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

   - the SIP URL identifying the P-CSCF;

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

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

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

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

5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the ‘sec-agree’ item from the Require header, and the header itself if this is the only entry.~~'Require: sec-agree' header shall also be removed~~. If the header is not present, then a suitable 4xx ~~error code~~response shall be sent back;

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

   - check the security association which protected the request. If that has a temporary lifetime, then the request shall contain a Security-Verify header. If there is no such header, then a suitable 4xx error code shall be sent back. If there is such header, then compare the content of the Security-Verify header with the local static security list. If those do not match, then there is a potential man-in-the-middle attack. The request should be rejected by sending a suitable 4xx ~~error~~ response. If the contents match, the~~n~~ P-CSCF shall remove the Security-Verify header, and the ‘sec-agree’ item from the Require header, and the header itself if this is the only entry~~together with the 'Require: sec-agree' header shall be removed from the request~~; and

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

   - check if the private user identity conveyed in the integrity-protected REGISTER request is the same as the private user identity which was previously challenged or authenticated. If the private user identities are different, the P-CSCF shall reject the REGISTER request by returning a 403 (Forbidden) response;

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

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

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

1) remove ~~and store~~ the CK and IK values contained in the 401 (Unauthorized) response and bind them to the proper private user identity and security association. The 401 (Unauthorized) response shall be forwarded to the UE if and only if the CK and IK have been removed;

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

3) set up the security association with a temporary lifetime between the UE and the P-CSCF for the user identified with the private user identity ~~with a temporary lifetime~~. For further details see 3GPP TS 33.203 [19] and draft-sip-sec-agree [48]. The SIP level lifetime of the Security Association shall be long enough to permit the UE to

finalize the registration procedure (bigger than 64*T1). The IPSec level lifetime of the Security Association shall be set to the maximum.

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

1) save the list of P-Service-Route headers preserving the order. This list shall be stored during the entire registration period of the respective public user identity. This list shall be used to preload the routeing information into the initial requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of P-Service-Route headers with the new list;

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

3) remove any Path and P-Service-Route headers from the 200 (OK) response before forwarding the response to the UE;

4) store the public user identities found in the P-Associated-URI header value, as those that are authorized to be used by the UE;

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

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

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

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

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

The P-CSCF shall delete any security association from the IPSec database when their SIP level lifetime expires.

3GPP TSG-CN1 Meeting #26 ***Tdoc N1-022084***
Miami Beach, Florida, USA, 23 – 27 September 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **212** ⌘ **rev** **1** ⌘ Current version: **5.2.0** ⌘

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

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

Title:	⌘	P-CSCF subscription to the users registration-state event
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	15/09/2002
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:	⌘	Incorrect text in the subclause 5.2.3 and incomplet information in the Note in the subclause 5.2.4.
Summary of change:	⌘	Corrected text and additional text in the Note indicating that there is an alternatwe method of discovering implicitly registered public user identities is provided.
Consequences if not approved:	⌘	Incorrect specification.

Clauses affected:	⌘	5.2.3 and 5.2.4			
Other specs affected:	⌘	**Y**	**N**		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	Revision 1 corrects the existing text by indicating that the Route header utilizes the service-route information and not path information. In addition, the proposed modification of the Note was rejected. However, new modification of the Note indicates that the P-CSCF receives the information and not the UE.			

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

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

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

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

5.2.3 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 reg event package at the users registrar (S-CSCF) as described in draft-rosenberg-sip-reg-00 [43]. Therefore the P-CSCF shall generate a SUBSCRIBE request with the following elements:

- a Request-URI set to the resource to which it wants to subscribe to, i.e. to a SIP URL of the public user identity that was previously registered~~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 "reg" 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 service-route~~path~~ information that was obtained during the users registration. ~~The 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 identities

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

- if a state parameter "active", 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 state parameter "terminated", 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 P-CSCF~~UE~~ about these automatically registered public user identities.

3GPP TSG-CN1 Meeting #26 ***Tdoc N1-022154***
Miami Beach, Florida, USA, 23 – 27 September 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **213** ⌘ **rev** **2** ⌘ Current version: **5.2.0** ⌘

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

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

Title:	⌘	Handling of MT call by the P-CSCF
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	15/09/2002
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:	⌘	Minor text corrections.
Summary of change:	⌘	Minor text corrections.
Consequences if not approved:	⌘	Incorrect text.

Clauses affected:	⌘	5.2.6.4

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

Other comments:	⌘	In Revision 2 the bullet 8 was added.

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

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

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

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

5.2.6.4 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:

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

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

3) save a copy of the Contact header received in the request~~response~~ in order to release the dialog if needed;

4) add itself on the top of the removed list of Record-Route headers and save the list. The list will be appended to any UE~~-~~originated 1xx or 2xx response to the ~~SUBSCRIBE~~ request;

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

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

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

8) save a copy of the P-Called-Party-ID header.

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

1) insert an P-Asserted-Identity header with a value representing the responder to the request. The responder shall be identified by the P-Called-Party-ID header that was received in the request;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3GPP TSG-CN1 Meeting #26 ***Tdoc N1-021939***
Miami Beach, Florida, USA, 23 – 27 September 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **215** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

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

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

Title:	⌘	P-CSCF acting as a UA
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	15/09/2002
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:	⌘	Incomplete specification of P-CSCF role.
Summary of change:	⌘	It is proposed to add information to clause 4,1 explaining that the P-CSCF acts as a UA when it performs a P-CSCF initiated dialog-release.
Consequences if not approved:	⌘	Incomplete specification.

Clauses affected:	⌘	4.1

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

Other comments: ⌘

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

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

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

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

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.

- The User Equipment (UE) shall provide the User Agent (UA) role with 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.~~Under certain circumstances as described in subclause 5.2, the P-CSCF shall provide the UA role with the additional capabilities, as follows:

  a) when acting as a subscriber to or the recipient of event information; and

  b) when performing P-CSCF initiated dialog-release the P-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.

- 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 dialog-release the S-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.

- The BGCF shall provide~~d~~ 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.

3GPP TSG-CN1 Meeting #26 ***Tdoc N1-022085***
Miami Beach, Florida, USA, 23 – 27 September 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **216** ⌘ **rev** **1** ⌘ Current version: **5.2.0** ⌘

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

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

Title:	⌘	S-CSCF handling of protected registrations
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	15/09/2002
Category:	⌘	**F**
Release:	⌘	*Rel-5*

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

Use one of the following releases:

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

Reason for change:	⌘	In case of multiple registrations, the REGISTER request for and unregistered public user identity will arrive as “integrity-protected” at the S-CSCF. Currently the 24.229 document does not clearly specify how to handle this case.
Summary of change:	⌘	The provided text describes the handling of the “integrity-protected” REGISTER request for and unregistered public user identity by the S-CSCF.
Consequences if not approved:	⌘	Incomplete specification.

Clauses affected:	⌘	5.4.1.2.2

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

Other comments:	⌘	Revision 1 incorporates the modifications requested by the working group.

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 reques

5.4.1.2.2 Protected REGISTER

Upon receipt of a REGISTER request with the integrity-protection parameter in the Authorization header set to ='yes', the S-CSCF shall identify the user by the public user identity as received in the To header and the private user identity as received in the Authorization header of the REGISTER request, and:

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

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

1~~2~~) check if the user needs to be reauthenticated.

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

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

2~~3~~) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in subclause 5.4.1.4. If the Expires header does not indicate zero, the S-CSCF shall check whether the public user identity received in the To header is already registered. If it is not registered, the S-CSCF shall proceed with the procedures as described for the second REGISTER request in subclause 5.4.1.2.2, beginning with step 5. Otherwise, the S-CSCF shall proceed with the procedures as described for the second REGISTER request in subclause 5.4.1.2.2~~,~~ beginning with step 6~~7~~).~~; and~~

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

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

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

1~~2~~) check if the Call-ID of the request matches with the Call-ID of the 401 (Unauthorized) response which carried the last challenge. The S-CSCF shall only proceed further if the Call-IDs match.

2~~3~~) stop timer reg-await-auth;

3~~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;

4~~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;

5~~6~~) after performing the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], store the following information in the local data:

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

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

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

6~~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.

7~~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.

8~~9~~) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may reduce the duration of the registration due to local policy or send back a 423 (Interval Too Brief) response specifying the minimum allowed time for registration;

9~~10~~) store the icid parameter received in the P-Charging-Vector header;

10~~1~~) remove the P-Access-Network-Info header and may act upon the contents accordingly;

11~~2~~) create a 200 (OK) response for the REGISTER request, including:

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

- the list of received Path headers;

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

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

- a P-Service-Route header containing:

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

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

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

12~~3~~) send the so created 200 (OK) response to the UE;

13~~4~~) 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.

14~~5~~) handle the user as registered for the duration indicated in the Expires header.