3GPP TSG CN Plenary Meeting #18 **NP-020561**
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 4**

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	239	1	F	Rel-5	Correction on P-Asserted-Id, P-Preferred-Id, Remote-Party-ID	N1-26	N1-022100	5.2.0
24.229	240	1	F	Rel-5	Clarifications to subclause 9.2.5	N1-26	N1-022137	5.2.0
24.229	242		F	Rel-5	ENUM translation	N1-26	N1-022020	5.2.0
24.229	243	1	F	Rel-5	AS routing	N1-26	N1-022107	5.2.0
24.229	245	1	F	Rel-5	Warning header	N1-26	N1-022108	5.2.0
24.229	246	3	F	Rel-5	S-CSCF procedure tidyup	N1-27	N1-022497	5.2.0
24.229	247	1	F	Rel-5	P-CSCF procedure tidyup	N1-26	N1-022125	5.2.0
24.229	248	2	F	Rel-5	UE procedure tidyup	N1-27	N1-022472	5.2.0
24.229	249	3	F	Rel-5	MESSAGE corrections part 1	N1-27	N1-022455	5.2.0
24.229	250	2	F	Rel-5	MESSAGE corrections part 2	N1-27	N1-022456	5.2.0

3GPP TSG-CN1#26 **Tdoc ⌘N1-022100**
Miami, Florida, 23-27 September 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **239** ⌘ **rev** **1** ⌘ Current version: **5.2.0** ⌘

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

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

Title:	⌘	Correction on P-Asserted-Identity, P-Preferred-Identity
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	17/09/2002
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:	⌘	Corrections according-to draft-ietf-asserted-identity-02
Summary of change:	⌘	Corrections according-to draft-ietf-asserted-identity-02
Consequences if not approved:	⌘	No IETF compliancy

Clauses affected:	⌘	5.1.2, 5.2.2, 5.2.6

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		24.228
			X	Test specifications		
			X	O&M Specifications		

Other comments: ⌘

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

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

5.1.2A Generic procedures applicable to all methods

5.1.2A.1 Mobile-originating case

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

- a public user identity stored in the USIM which has been registered by the user;
- a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implict registration that was not subsequently deregistered or has expired; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

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

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

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

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

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

5.1.2A.2 Mobile-terminating case

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

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

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

5.1.3 Call initiation - mobile originating case

5.1.3.1 Initial INVITE

Upon generating an initial INVITE request, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism;
- indicate the requirement of precondition and specify it using the Require header mechanism.

If the UA receives a 503 (Service Unavailable) response to an initial INVITE request containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

5.1.4 Call initiation - mobile terminating case

5.1.4.1 Initial INVITE

Upon receiving an initial INVITE request without containing either Supported: precondition or Require: precondition header values, the UE shall generate a 421 (Extension Required) response indicating the required extension in the Require header field.

Upon generating the first response to the initial INVITE request, the UE shall indicate the requirement for reliable provisional responses and specify it using the Require header mechanism.The UE shall send the 200 (OK) response to the initial INVITE request only after the local resource reservation has been completed.

5.1.5 Call release

Void.

5.1.6 Emergency service

A UE shall not attempt to establish an emergency session via the IM CN Subsystem when the UE can detect that the number dialled is an emergency number. The UE shall use the CS domain as described in 3GPP TS 24.008 [8].

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a XML body that includes an <alternative service> element with the <type> child element set to "emergency", the UE shall automatically:

- send an ACK request to the P-CSCF as per normal SIP procedures;
- attempt an emergency call setup according to the procedures described in 3GPP TS 24.008 [8].

The UE may also provide an indication to the user based on the text string contained in the <reason> element.

As a consequence of this, a UE operating in MS operation mode C cannot perform emergency calls.

5.1.7 MESSAGE support

The UE shall support the SIP MESSAGE method described in draft-ietf-sip-message-06 [50]. A UE shall be capable of sending and receiving MESSAGE method to conduct session-unrelated or session-related interactions. To do so, a UE may either initiate or terminate MESSAGE requests per draft-ietf-sip-message-06.txt [50]. The UE should support, as a minimum, a body of type "text/plain" per draft-ietf-sip-message-06.txt [50].

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

5.2 Procedures at the P-CSCF

5.2.1 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.

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 user's 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 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 path information that was obtained during the users registration. Th S-CSCF shall set the last Route header entry to the resource to which it wants to subscribe to, i.e. to a SIP URL the public user identity that was previously registered.

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

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

5.2.4 Registration of multiple public user identites

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the 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 UE about these automatically registered public user identities.

5.2.5 Deregistration

5.2.5.1 User-initiated deregistration

When the P-CSCF receives a 200 (OK) response to a REGISTER request (sent according to subclause 5.2.2), it shall check the value of the Expires header field and/or expires parameter in the Contact header field. When the value of the Expires header field or expires parameter equals zero, then the P-CSCF shall:

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

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

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

5.2.5.2 Network-initiated deregistration

If the P-CSCF:

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

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

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

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

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

5.2.6.1 Introduction

The procedures of subclause 5.2.6 and its subclauses are general to all requests and responses, except those for the REGISTER method.

5.2.6.2 Determination of mobile-originated or mobile-terminated case

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

- perform the procedures for the mobile-terminating case as described in subclause 5.2.6.4 if the request makes use of the information for mobile-terminating calls, which was added to the Path header entry of the P-CSCF during registration (see subclause 5.2.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter;

- perform the procedures for the mobile-originating case as described in subclause 5.2.6.3 if this information is not used by the request.

5.2.6.3 Requests initiated by the UE

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

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

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

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

1) remove any Route header from the request;

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

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

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

5) re~~place~~move the P-Preferred-Identity header, if present, ~~with~~insert~~and insert~~ a P-Asserted-Identity header with a value representing the initiator of the request;

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

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

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

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

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

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

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

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

6) forward the response to the UE.

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

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

2) forward the response to the UE.

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

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

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

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

2) remove any Route header from the request;

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

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

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

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

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

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

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

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

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

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

2) forward the response to the UE.

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

1) remove any Route header from the request;

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

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

4) remove the P-Preferred-Identity header, if present, and insert ~~replace the P-Preferred-Identity header with~~ insert a P-Asserted-Identity header with a value representing the initiator of the request;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2) forward the response to the UE.

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

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

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

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

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

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

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

3) remove the P-Preferred-Identity header, if present, and insert a~~replace the P-Preferred-Identity header with insert an~~ P-Asserted-Identity header with a value representing the initiator of the request; and

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

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

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

2) forward the response to the UE.

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

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

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

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

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

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

1) remove the P-Preferred-Identity header, if present, and ~~replace the P-Preferred-Identity header wit~~insert a~~n~~ P-Asserted-Identity header with the~~a~~ value saved from Request-URI of the request~~representing the responder to the request~~;

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

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

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

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

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

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

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

~~2~~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;

~~3~~2) store the values received in the P-Charging-Function-Addresses header; and

~~4~~3) 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) remove the P-Preferred-Identity header, if present, and insert an P-Asserted-Identity header with the value saved from Request-URI of the request~~remove the P-Preferred-Identity header, if present~~;~~—~~

2) 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 N1-022137***
Miami Beach, Florida, USA, 23 – 27 September 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **240** ⌘ **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:	⌘	Clarifications to subclause 9.2.5
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	23/09/2002
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 name of RFC 3313 is corrected. It is clarified that the media authorization token is transparently conveyed in the UE on a byte-by-byte basis. The term media authorization token is consistantly used throughout clause 9. The names for the GPRS procedures are corrected. It is clarified that the IMS signalling flag cannot be set on a PDP context for media.
Summary of change:	⌘	Clarifications regarding the use of the media authorization token by the UE. Various clarifications and corrections.
Consequences if not approved:	⌘	The detailed description of the use of the media authorization token will not be complete and consistant.

Clauses affected:	⌘	2, 9.2.5

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

Other comments:	⌘	

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

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

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

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

********** 1st modification **********

2 References

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

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

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

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

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

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

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

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

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

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

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

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

[10A] 3GPP TS 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): "Private SIP ~~e~~Extensions for ~~m~~Media ~~a~~Authorization".

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[46] Void.

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

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

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

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

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

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

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

********** 2nd modification **********

9 GPRS aspects when connected to the IM CN subsystem

9.1 Introduction

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

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

9.2 Procedures at the UE

9.2.1 PDP context activation and P-CSCF discovery

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure;

b) establish a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A]. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv6 address;

   The UE shall choose one of the following options when performing establishment of this PDP context:

   I. A dedicated PDP context for SIP signalling:

      The UE shall indicate to the GGSN that this is a PDP context intended to carry IM CN subsystem-related signalling only by setting the IM CN Subsystem Signalling Flag. The UE may also use this PDP context for DNS and DHCP signalling according to the static packet filters described in 3GPP TS 29.207 [12];

   II. A general-purpose PDP context:

      The UE may decide to use a general-purpose PDP Context to carry IM CN subsystem-related signaling. The UE shall indicate to the GGSN that this is a general-purpose PDP context by not setting the IM CN Subsystem Signalling Flag. The UE may carry both signalling and media on the general-purpose PDP context.

   The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

   Detailed description of how the IM CN Subsystem Signalling Flag is carried in the Protocol Configuration Options IE is provided in 3GPP TS 24.008 [8].

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

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

   The methods for P-CSCF discovery are:

I. Employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) draft-ietf-dhc-dhcpv6 [40], the DHCPv6 options for SIP servers draft-ietf-sip-dhcpv6 [41] and if needed DNS after PDP context activation.

   The UE shall either:

   - in the DHCP query, request a list of SIP server domain names of P-CSCF(s) and the list of Domain Name Servers (DNS); or

   - request a list of SIP server IPv6 addresses of P-CSCF(s).

II. Transfer P-CSCF address(es) within the PDP context activation procedure.

   The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options IE of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

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

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

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

The UE may request a DNS Server IPv6 address(es) via draft-ietf-dhc-dhcpv6-26 [40] or by the Protocol Configuration Options IE when activating a PDP context according to 3GPP TS 27.060 [10A].

Detailed description of how the request and response for IPv6 address(es) for DNS server(s) and list of P-CSCF address(es) are carried in the Protocol Configuration Options IE is provided in 3GPP TS 24.008 [8].

9.2.1A Modification of a PDP context used for SIP signalling

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

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

9.2.1B Re-establishment of the PDP context for signalling

If the dedicated PDP context for SIP signalling is lost due to e.g. a GPRS routeing area update procedure, the UE shall attempt to re-establish the dedicated PDP context for SIP signalling. If this procedure does not succeed, the UE shall deactivate all PDP contexts related to IMS.

9.2.2 Session management procedures

The existing procedures for session management as described in 3GPP TS 24.008 [8] shall apply while the UE is connected to the IM CN subsystem.

9.2.3 Mobility management procedures

The existing procedures for mobility management as described in 3GPP TS 24.008 [8] shall apply while the UE is connected to the IM CN subsystem.

9.2.4 Cell selection and lack of coverage

The existing mechanisms and criteria for cell selection as described in 3GPP TS 25.304 [9] and 3GPP TS 44.018 [20] shall apply while the UE is connected to the IM CN subsystem.

9.2.5 PDP contexts for media

The UE shall establish different PDP contexts for media streams that belong to different SIP sessions.

During establishment of a session, the UE establishes data streams(s) for media related to the session. Such data stream(s) may result in activation of additional PDP context(s). Such additional PDP context(s) shall be established as secondary PDP contexts associated to the PDP context used for signalling.

The P-CSCF shall indicate to the UE in SIP/SDP if a separate PDP Context is required for a media component as per procedures defined in 3GPP TS 23.228 [7]. The UE shall establish an additional PDP context for a media component if so indicated by the P-CSCF.

The UE shall transparently pass the media authoriz~~s~~ation token received from the P-CSCF in the 183 (Session Progress) response to an INVITE request at originating setup or in the INVITE request at terminating setup to the GGSN. The UE shall ~~be~~ signal it ~~by inserting it~~ within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message ~~at PDP Context activation/modification~~.

~~In order t~~To identify to the GGSN which flow(s) (identified by m-lines within the SDP) that are ~~to be~~ transferred within a particular PDP context, the UE shall set the flow identifier(s) within the Traffic Flow Template IE in the ACTIVATE SECONDARY PDP CONTEXT REQUEST message or the MODIFY PDP CONTEXT REQUEST message~~at PDP Context activation modification~~. Detailed description of how the flow identifiers are constructed is provided in 3GPP TS 29.207 [12].

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

The UE shall not include the IM CN Subsystem Signalling Flag when a PDP context for media is established or modified.

3GPP TSG-CN1 Meeting #26 ***Tdoc N1-022020***
Miami Beach, Florida, USA, 23 – 27 September 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **242** ⌘ **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 ☒

Title:	⌘	ENUM translation
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	17/09/2002
Category:	⌘	**F**
Release:	⌘	R5

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:	⌘	When ENUM translation fails it is not possible to evaluate initial filter criteria and visit one or more AS. The visit to an AS may be needed e.g. to modify the number.
Summary of change:	⌘	ENUM translation can be done after visiting application servers.
Consequences if not approved:	⌘	It is not possible to evaluate initial filter criteria when ENUM translation fails.

Clauses affected:	⌘	5.4.3.2

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

Other comments: ⌘

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

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

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

5.4.3.2 Requests initiated by the served user

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

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

- remove its own SIP URL from the topmost Route header;

- ~~if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [22]) to a globally routeable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or an appropriate SIP response shall be sent to the originator;~~

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

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

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

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

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

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

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

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

- <u>if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [22]) to a globally routeable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or an appropriate SIP response shall be sent to the originator;</u>

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

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

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

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

- route the request based on SIP routeing procedures.

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

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

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

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

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

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

- remove its own URL from the topmost Route header;

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

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

- route the request based on the topmost Route header.

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

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

- remove its own URL from the topmost Route header;

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

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

- route the request based on the topmost Route header.

3GPP TSG-CN1#26 **Tdoc ⌘N1-022107**
Miami, Florida, 23-27 September 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **243** ⌘ **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:	⌘	AS routing
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	15/07/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

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

Use one of the following releases:

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

Reason for change:	⌘	It is not specified how the AS finds out the correct S-CSCF to send the message to.
Summary of change:	⌘	Clarification added on how to obtain the address of the S-CSCF into 5.7.3. The procedures in 5.7.3 should be applied for all initiated requests, not only INVITE.
Consequences if not approved:	⌘	There would not be a way how the AS finds out the correct S-CSCF to send the message to.

Clauses affected:	⌘	5.7.3, 5.7.5.5

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

Other comments: ⌘

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

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

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

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

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

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

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

5.7.3 Application Server (AS) acting as originating UA

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

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

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

Furthermore the AS shall insert a Route header pointing to the S-CSCF of the UE on whose behalf the request is generated.

Note: The address of the S-CSCF may be obtained either from a previous request terminated by the AS, ~~or~~ by querying the HSS on the Sh interface or from static configuration.~~.~~

5.7.4 Application Server (AS) acting as a SIP proxy

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

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

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

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

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

5.7.5.1 General

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

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

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

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

5.7.5.2 Call initiation

5.7.5.2.1 Initial INVITE

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

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

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

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

5.7.5.2.2 Subsequent requests

Void.

5.7.5.3 Call release

5.7.5.4 Call-related requests

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

5.7.5.5 Further initial requests

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

~~Void~~.

3GPP TSG-CN1#26 **Tdoc ⌘N1-022108**
Miami, Florida, 23-27 September 2002

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **245** ⌘ **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:	⌘	Warning header
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	15/07/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

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

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

Reason for change:	⌘	The inclusion of Warning headers in 403 responses is randomly specified. This CR includes in all necessary places the requirement to include a Warning header with the specific reason of rejection of a request.
Summary of change:	⌘	Warning headers need to be included in 403 responses whenever is suitable. The missing text is added into the TS. The warn-code to be used is 399, as agreed while discussing the N1-021263.
Consequences if not approved:	⌘	Random usage of Warning headers.

Clauses affected:	⌘	5.2.6.3, 5.3.1.3, 5.4.1.2.1, 5.4.1.4, 5.4.3.2

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

Other comments:	⌘	

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

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

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

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

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

5.2.6.3 Requests initiated by the UE

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

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

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

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

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

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

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

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

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

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

1) verify if the request relates to a dialog in which the originator of the request is involved:
   a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response ~~shall~~may include a Warning header containing the warn-code 399~~ and an explanatory warn-text~~. The P-CSCF will not forward the request. No other actions are required;
   b) if the request relates to an existing dialog in which the originator is involved, then the P-CSCF shall continue with the following steps;

2) remove any Route header from the request;

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

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

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

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

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

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

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

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

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

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

2) forward the response to the UE.

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

1) remove any Route header from the request;

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

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

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

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

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

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

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

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

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

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

   a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response ~~shall~~may include a Warning header containing the warn-code 399 ~~and an explanatory warn-text~~ .The P-CSCF will not forward the request. No other actions are required;

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

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

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

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

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

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

2) forward the response to the UE.

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

1) send a 403 (Forbidden) response back to the UE ~~containing a warning header.~~. The response ~~shall~~may include a Warning header containing the warn-code 399 ~~and an explanatory warn-text~~.

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

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

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

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

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

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

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

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

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

2) forward the response to the UE.

5.3.1.3 Abnormal cases

In the case of SLF query, if the SLF does not send HSS address to the I-CSCF, the I-CSCF shall send back a 403 (Forbidden) response to the UE. The response ~~shall~~may include a Warning header containing the warn-code 399 ~~and an explanatory warn-text~~.

If the HSS sends a negative response to the user registration status query request, the I-CSCF shall send back a 403 (Forbidden) response. The response ~~shall~~may include a Warning header containing the warn-code 399 ~~and an explanatory warn-text~~.

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

If a selected S-CSCF:

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

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

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

5.4.1.2.1 Unprotected REGISTER

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

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

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

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

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

4) check how many authentications are ongoing for this user. The S-CSCF may – based on local policy – reject the request by sending a 403 (Forbidden) response, if there are a number of ongoing authentications. The response ~~shall~~may include a Warning header containing the warn-code 399 ~~and an explanatory warn-text.~~ If the S-CSCF decides to challenge the user, then proceed as follows;

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

   Prior to performing Cx Multimedia Authentication procedure with the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14];

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

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

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

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

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

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

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

5.4.1.4 User-initiated deregistration

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

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

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

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

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

If the Authorization header of the REGISTER request did not contain an Integrity-protection parameter, or the parameter was set to the value 'no', the S-CSCF shall respond to the request with a 403 (Forbidden) response. The response may contain a Warning header with a warn-code 399 ~~and an explanatory warn-text~~ ~~with the reason of rejecting the request~~.

5.4.3.2 Requests initiated by the served user

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

- determine whether the request contains a barred public user identity in the From or Remote-Party-ID header fields of the request or not. In case any of the said header fields contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. The response ~~shall~~ may include a Warning header containing the warn-code 399 ~~and an explanatory warn-text.~~ Otherwise, continue with the rest of the steps;

- remove its own SIP URL from the topmost Route header;

3GPP TSG-CN1 Meeting #27 ***Tdoc N1-022497***
Bangkok, Thailand, USA, 11 – 15 November 2002

was Tdoc N1-022032, Tdoc N1-022147, Tdoc N1-022371

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **246** ⌘ **rev** **3** ⌘ 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:	⌘	S-CSCF procedure tidyup
Source:	⌘	Dynamicsoft, Lucent
Work item code:	⌘	IMS-CCR
Date:	⌘	10/30/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

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

Use one of the following releases:

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

Reason for change:	⌘	Removal of possibility for S-CSCF to modify from header and correction of text into style of remaining document
Summary of change:	⌘	Deletion of from header modification step in clause 5.4.3.2 Missing names of responses included in parentheses after response status-code. Conversion of sentences from passive to active to improve clarity. Numbering of unnumbered lists, and adding "and" to penultimate item. Minor restructure of Note 1 of clause 5.4.1.2.1. Insertion of correct package name in 5.4.1.5. Minor restructure of items in 5.4.1.7. Removal of instance of Remote-Party-ID in 5.4.3.2.
Consequences if not approved:	⌘	Non compliance with RFC 3261 procedures and lack of readability in document due to inconsistency of style.

Clauses affected:	⌘	5.4.1.2.1, 5.4.1.2.2, 5.4.1.5, 5.4.1.7, 5.4.3.2, 5.4.4.2.1, 5.4.4.2.2, 5.4.6.1.2, 5.4.6.1.3

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

Other comments:	⌘	Revision 3 of this CR created to remove interaction with CR 264R1 in clause 5.4.4.2.1 and 5.4.4.2.2

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

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

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

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

FIRST PROPOSED CHANGE

5.4.1.2.1 Unprotected REGISTER

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

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

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

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

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

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

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

   Prior to performing Cx Multimedia Authentication procedure with the HSS, the S-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14];

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

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

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

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

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

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

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

5.4.1.2.2 Protected REGISTER

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

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

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

2) check if the user needs to be reauthenticated.

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

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

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

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

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

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

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

3) stop timer reg-await-auth;

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

   a) the private user identity of the user in the username field;

   b) the algorithm which is AKAv1-MD5 in the algorithm field; and

   c) the RES parameter needed for the authentication procedure in the response field.

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

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

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

   a) 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,

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

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

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

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

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

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

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

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

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

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

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

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

~~-~~b) the list of received Path headers;

~~-~~c) 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.

~~-~~d) 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~~ are ~~expected be~~ treated as for the mobile-originating case. This indication may e.g. be in a URI parameter, a character string in the user part or be a port number;
- if network topology hiding is required a SIP URL identifying an I-CSCF(THIG) as the topmost entry;

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

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

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

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

SECOND PROPOSED CHANGE

5.4.1.5 Network-initiated deregistration

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

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

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

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

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

THIRD PROPOSED CHANGE

5.4.1.7 Notification of Application Servers about registration status

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

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

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

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

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

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

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

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

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

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

FOURTH PROPOSED CHANGE

5.4.3.2 Requests initiated by the served user

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

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

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

3) if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [22]) to a globally routeable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response ~~shall be sent~~ to the originator;

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

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

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

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

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

8) 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;

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

~~10) in the case where the network operator has policy to provide privacy on From headers, and such privacy is required for this dialog, change the From header to "Anonymous". Network policy may also require the removal of the display field;~~

10~~1~~) determine the destination address (e.g. DNS access) using the URL placed in the topmost Route header if present, otherwise based on the Request-URI;

11~~2~~) if network hiding is needed due to local policy, put the address of the I-CSCF(THIG) to the topmost route header;

-123) in case of an initial request for a dialog the S-CSCF shall create a Record-Route header containing its own SIP URL and save the necessary Record-Route header fields and the Contact header from the request in order to release the dialog when needed;

-134) remove the P-Access-Network-Info header and act upon the contents accordingly; and

-145) route the request based on SIP routeing procedures.

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

-1) apply any privacy required by RFC 3323 [33] to the P-Asserted-Identity header.

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

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

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

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

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

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

-3) remove the P-Access-Network-Info header and act upon the contents accordingly; and

-4) route the request based on the topmost Route header.

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

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

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

-2) remove the P-Access-Network-Info header and act upon the contents accordingly;

-3) remove the P-access-network-info header and act upon the contents accordingly; and

-4) route the request based on the topmost Route header.

FIFTH PROPOSED CHANGE

5.4.4.2.1 Mobile-originating case

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

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

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

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

5.4.4.2.2 Mobile-terminating case

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

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

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

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

SIXTH PROPOSED CHANGE

5.4.6.1.2 Mobile-originating case

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

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

5.4.6.1.3 Mobile-terminating case

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

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

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

Tdoc N1-022125

was Tdoc N1-022033

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **247** ⌘ **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:	⌘	P-CSCF procedure tidyup
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	17/09/2002
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:	⌘	Correction of text into style of remaining document
Summary of change:	⌘	Conversion of sentences from passive to active to improve clarity. Restructure of forward request/response text in 5.2.6.3 and 5.2.6.4.
Consequences if not approved:	⌘	Lack of readability in document due to inconsistency of style.

Clauses affected:	⌘	5.2.2, 5.2.6.3, 5.2.6.4

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

Other comments:	⌘	For r1 version, changes to 5.2.7.4 have been removed to avoid interaction of CRs.

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

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

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

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

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

FIRST PROPOSED CHANGE

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~~ are expected to 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 the P-CSCF shall return 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 the P-CSCF shall return 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 P-CSCF shall remove 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 Security-Verify header is present, then the P-CSCF shall remove that header ~~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 P-CSCF shall forward 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 P-CSCF shall set the SIP level lifetime of the Security Association ~~shall~~ to be long enough to permit the UE to finalize the registration procedure (bigger than 64*T1). The P-CSCF shall set 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. The P-CSCF shall store ~~This~~ this list ~~shall be stored~~ during the entire registration period of the respective public user identity. The P-CSCF shall use ~~This~~ 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.

SECOND PROPOSED CHANGE

5.2.6.3 Requests initiated by the UE

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

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

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

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

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

~~7) forward the request based on the topmost Route header.~~

before forwarding the request, ~~(~~based on the topmost Route header,~~)~~ in accordance with the procedures of RFC 3261 [26].

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

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

~~6) forward the response to the UE.~~

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

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

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

~~2) forward the response to the UE.~~

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

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

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

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

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

2) remove any Route header from the request;

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

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

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

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

before forwarding the request, (based on the topmost Route header,) in accordance with the procedures of RFC 3261 [26].

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

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

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

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

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

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

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

2) forward the response to the UE.

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

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

1) remove any Route header from the request;

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

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

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

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

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

before forwarding the request, (based on the topmost Route header,) in accordance with the procedures of RFC 3261 [26].

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

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

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

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

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

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

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

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

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

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

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

before forwarding the request to the UE, ~~(~~based on the topmost Route header,~~)~~ in accordance with the procedures of RFC 3261 [26].

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

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

~~2) forward the response to the UE.~~

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

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

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

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

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

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

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

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

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

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

before forwarding the request, ~~(~~based on the topmost Route header,~~)~~ in accordance with the procedures of RFC 3261 [26].

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

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

~~2) forward the response to the UE.~~

before forwarding the response to the UE in accordance with the procedures of RFC 3261 [26].

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 the 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 the Contact header received in the response in order to release the dialog if needed;
4) add itself on the top of the removed list of Record-Route headers and save the list. The list will be appended to UE originated response to the SUBSCRIBE request;
5) remove and store the list of received Via headers from the received request and shall place its own address in the Via header with locally unique token to identify the saved values as a branch parameter. The P-CSCF shall append the list of Via headers to the UE originated response for this request;
6) store the values received in the P-Charging-Function-Addresses header; and
7) remove and store the icid parameter received in the P-Charging-Vector header;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

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

1) insert an P-Asserted-Identity header with a value representing the responder to the request;
2) append the saved list of Record-Route headers to the response;
3) append the saved list of Via headers to the response; and
4) store the dialog ID and associate it with the private user identity and public user identity involved in the session;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

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;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

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;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

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;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

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;

before forwarding the request to the UE in accordance with the procedures of RFC 3261 [26].

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;

before forwarding the response in accordance with the procedures of RFC 3261 [26].

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

Tdoc N1-022472

was Tdoc N1-022034

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **248** ⌘ **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 procedure tidyup
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	17/09/2002
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:	⌘	Collision of CRs.~~Correction of text into style of remaining document~~
Summary of change:	⌘	~~Conversion of sentences from passive to active to improve clarity.~~ ~~Clarification of meaning of final paragraph of 5.1.1.1A.~~ ~~Insertion of name of response.~~ ~~Alignment of 5.1.1.4 and 5.1.1.6 text with 5.1.1.2.~~ One change which changes passive voice to active, has been reversed and the change has been included in another CR.
Consequences if not approved:	⌘	Problems implementing the CRs. ~~Lack of readability in document due to inconsistency of style.~~

Clauses affected:	⌘	5.1.1.1A, 5.1.1.4, 5.1.1.5.1, 5.1.1.6
Other specs affected:	⌘	Y N ☐ ☒ Other core specifications ☐ ☒ Test specifications ☐ ☒ O&M Specifications
	⌘	
Other comments:	⌘	

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

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

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

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

5.1 Procedures at the UE

5.1.1 Registration and authentication

5.1.1.1 General

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

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

5.1.1.1A Parameters contained in the UICC

In case the UE is loaded with a UICC that contains the ISIM application, it will be preconfigured with all the necessary parameters to initiate the registration to the IM CN subsystem. These parameters include:

- the private user identity;
- one ore more public user identities; and
- the home network domain name used to address the SIP REGISTER request

In case the UE is loaded with a UICC that does not contain the ISIM application, the UE shall:

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to.

All these three parameters are derived from the IMSI parameter in the USIM, according to the procedures described in 3GPP TS 23.003 [3]. If ~~a~~ the ~~UE is loaded with a~~ UICC ~~that~~ does not contain the ISIM application, the UE shall derive new values every time the UICC is changed, and shall discard existing values if the UICC is removed.

The temporary public user identity is only used in REGISTER requests. After a successful registration, the UE will get the associated public user identities, and the UE may use any of them ~~shall be used~~ in subsequent non-REGISTER messages.

As the temporary public user identity may be barred, the UE shall not reveal the temporary public user identity to the user.

~~In the case the UE needs to derive the temporary public user identity, the procedure shall be executed every time the UICC is changed.~~

5.1.1.2 Initial registration

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.1.1.3 Initial subscription to the registration-state event package

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the users reg event package for the public user identity registered as described in subclause 5.1.1.2 at the users registrar (S-CSCF). The reg event package is described in draft-rosenberg-sip-reg-00 [43]. Therefore the UE shall generate a SUBSCRIBE request with the following elements:

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

- a From header set to a SIP URL that contains a public user identity;

- a To header, set to a SIP URL that contains a public user identity;

- an Event header set to the "reg" event package;

- an Expires header set to a value higher than the Expires header of the before sent REGISTER request.

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

Afterwards it shall send out the so generated SUBSCRIBE request.

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

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

5.1.1.4 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 UE shall integrity protect the REGISTER request ~~shall be integrity protected~~ using IK, see 3GPP TS 33.203 [19], ~~received~~ derived as a result of ~~in~~ an earlier registration, if IK is available.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5.1.1.5 Authentication

5.1.1.5.1 General

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

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

- check the validity of a received authentication challenge, as described in 3GPP TS 33.102 [18] i.e. the locally calculated MAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

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

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

- extract the RAND and AUTN parameters, and use the derived keys (CK and IK) to protect future messages, see 3GPP TS 33.203 [19]; and

- send another REGISTER request using the derived IK to integrity protect the message. The header fields are populated as defined for the initial request, with the addition that the UE shall include an Authorization header containing the private user identity and the authentication challenge response (RES parameter). Instead of the Security-Client header the UE shall insert the Security-Verify header into the request, by mirroring in it the content of the Security-Server header received in the 401 (Unauthorized) response. The Call-ID of the integrity protected REGISTER request which carries RES must be the same as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

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

5.1.1.5.2 Network-initiated re-authentication

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

5.1.1.5.3 Abnormal cases

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

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no response parameter (e.g. no RES or AUTS);

- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the AUTS parameter (see 3GPP TS 33.102 [18]).

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

5.1.1.6 Mobile-initiated deregistration

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

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

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

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

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

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

The UE shall 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 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 UE shall integrity protect the REGISTER request ~~shall be sent integrity protected~~ using IK, see 3GPP TS 33.203 [19], derived as a result of an earlier registration, if IK is available.

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

5.1.1.7 Network-initiated deregistration

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.1.2.1, which contains the state parameter set to "terminated" and the event parameter "rejected", i.e. deregistered, for one or more public user identities that were previously stored as registered, the UE shall remove all registration details relating to these public user identities.

3GPP TSG-CN1 Meeting #26 ***Tdoc N1-022455***
Bangkok, Thailand, 11 – 15 November 2002

was Tdoc N1-022035, Tdoc N1-022346

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **249** ⌘ **rev** **3** ⌘ 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:	⌘	MESSAGE corrections part 1
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	17/09/2002
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: ⌘ At the last meeting, changes were made to 24.229 to introduce the MESSAGE method for ther delivery of application server information between AS and UE, and for the delivery of information between UEs, as required in subclause 5.4.9 of TS 23.228. It is considered that a number of these changes were made in such a manner to cause confusion on the support of other capabilities that are only specified in Annex A. Additionally, material should have been included in Annex to support this method, and this material was missing from the original CR.
In particular, it appears the text dealing with the length of the MESSAGE method is: i) common to the handling of all methods, and not specific to the MESSAGE method; ii) is already specified for all methods within clause 18 of RFC 3261. Rather than duplicating the RFC in this respect, it would appear appropriate to find a general location to provide a pointer to the RFC 3261 text. A new clause 4.2A is proposed to resolve this. This does however introduce a technical change, as the current text within 24.229 specifies the usage of TCP, and the change reverts to the rather more general text in RFC 3261 " the request MUST be sent using an RFC 2914 [43] congestion controlled transport protocol, such as TCP". If both sides support SCTP, then SCTP could be used rather than TCP. The support of TCP by all entities is mandatory so this is the common denominator.

Summary of change: ⌘
- In clause 4.1, additions have been made to the S-CSCF to indicate that it is providing UA functionality for the MESSAGE method usage.
- The contents of the new clause 5.1.7 are deleted. This material contains two paragraphs, the first contains mandatory requirements reproduced from the MESSAGE draft. The second paragraph is a mandatory requirement of RFC

		3261 for ALL method, not specifically the MESSAGE method. Explicit specification for the MESSAGE method implies that it does not apply to other methods. • The contents of the new clause 5.2.11 are deleted. The clause is a mandatory requirement of RFC 3261 for ALL method, not specifically the MESSAGE method. Explicit specification for the MESSAGE method implies that it does not apply to other methods. • The contents of the new clause 5.3.4 are deleted. The clause is a mandatory requirement of RFC 3261 for ALL method, not specifically the MESSAGE method. Explicit specification for the MESSAGE method implies that it does not apply to other methods. • The contents of the new clause 5.4.7 are modified. The first paragraph is only possible with the S-CSCF is acting as a UA, and therefore it is assumed to be possible only when the S-CSCF is acting outside of a dialog. The text has therefore been modified to reflect this. A related addition has therefore also been made to clause 4.1. The second paragraph is a mandatory requirement of RFC 3261 for ALL method, not specifically the MESSAGE method. Explicit specification for the MESSAGE method implies that it does not apply to other methods. • The contents of the new clause 5.7.6 are deleted. Firstly the procedures are only possible when the AS is acting as a UA, and not as a proxy (as described in clause 5.7.4), or as a redirect server (as described in part of clause 5.7.2), and therefore even if included they should be included explicitly under the remaining clauses. This material contains two paragraphs, the first contains mandatory requirements reproduced from the MESSAGE draft. The second paragraph is a mandatory requirement of RFC 3261 for ALL method, not specifically the MESSAGE method. Explicit specification for the MESSAGE method implies that it does not apply to other methods.
Consequences if not approved:	⌘	By using a different manner of specification for a mandatory method to that used for other mandatory methods, confusion is cast on the support for those methods.

Clauses affected:	⌘	4.1, 4.2A (new), 5.1.7, 5.2.11, 5.3.4, 5.4.7, 5.7.6			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘	Note that the change to clause 4.1 may interact with N1-022261 and may need to be redrafted if that contributions is approved.			

How to create CRs using this form:

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

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

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

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

FIRST PROPOSED CHANGE

4.1 Conformance of IM CN subsystem entities to SIP

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

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

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

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

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

- The User Equipment (UE) shall provide the User Agent (UA) rolewith the exceptions and additional capabilities as described in subclause 5.1.

- The P-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.2. When acting as the subscriber to or the recipient of event information, the P-CSCF shall provide the UA role, again with the exceptions and additional capabilities as described in subclause 5.2.

- The I-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.3.

- The S-CSCF shall provide the proxy role, with the exceptions and additional capabilities as described in subclause 5.4. Under certain circumstances as described in subclause 5.4, the S-CSCF shall provide the UA role with the additional capabilities, as follows:

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

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

  c) when providing a messaging mechanism by ~~as a source of information to the user by~~ sending the MESSAGE method, the S-CSCF shall provide the UA role; and

  d~~e~~) when performing S-CSCF initiated release the S-CSCF shall provide the UA role, even when acting as a proxy for the remainder of the dialog.

- The BGCF shall provided the proxy role, with the exceptions and additional capabilities as described in subclause 5.5.

- The MGCF shall provide the UA role, with the exceptions and additional capabilities as described in subclause 5.6.

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

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

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

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

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

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

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

SECOND PROPOSED CHANGE - NEW CLAUSE 4.2A

4.2A Transport mechanisms

This document makes no requirement on the transport protocol used to transfer signalling information over and above that specified in RFC 3261 [26] clause 18. ~~In particular, the path maximum transmission unit is unknown within the IM CN subsystem, and therefore the UE and IM CN subsystem entities shall transport SIP messages longer than 1300 bytes according to the procedures of RFC 3261 [26] clause 18.1.1.~~However, the UE and IM CN subsystem entities shall transport SIP messages longer than 1300 bytes according to the procedures of RFC 3261 [26] clause 18.1.1, even if a mechanism exists of discovering a maximum transmission unit size longer tha 1500 bytes.

THIRD PROPOSED CHANGE

5.1.7 ~~MESSAGE support~~Void

~~The UE shall support the SIP MESSAGE method described in draft-ietf-sip-message-06 [50]. A UE shall be capable of sending and receiving MESSAGE method to conduct session-unrelated or session-related interactions. To do so, a UE may either initiate or terminate MESSAGE requests per draft-ietf-sip-message-06.txt [50]. The UE should support, as a minimum, a body of type "text/plain" per draft-ietf-sip-message-06.txt [50].~~

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

FOURTH PROPOSED CHANGE

5.2.11 ~~MESSAGE support~~Void

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

FIFTH PROPOSED CHANGE

5.3.4 ~~MESSAGE support~~Void

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

SIXTH PROPOSED CHANGE

5.4.7 MESSAGE support

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

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

SEVENTH PROPOSED CHANGE

5.7.6 ~~MESSAGE support~~Void

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

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

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

Tdoc N1-022456

was Tdoc N1-022347

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **250** ⌘ **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:	⌘	MESSAGE corrections part 2
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	02/11/02
Category:	⌘	**F**
Release:	⌘	Rel-5

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

Use one of the following releases:

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

Reason for change:	⌘	Previous CRs that introduced the MESSAGE method provided only a single table within the Annex A profile whose contents were inconsistent with the remainder of the profile. There were also a number of errors, and the proxy role entry was missing altogether. This CR provides a set of tables consistent with the status of the remainder of the Annex A profile.
Summary of change:	⌘	• In the UA role, new tables are introduced to represent the various responses that can occur to the MESSAGE method. • New tables are introduced for the proxy role, with amendments to the major capabilitys and methods table to introduce the MESSAGE extension and MESSAGE method. • The contents of discussion documents N1-022325 - N1-022343 have been taken into account in completing these tables, consistent with the CR contained in N1-022344 which provides this information in the tables for other methods. • References in the existing request table have been revised. • The remaining headers in the tables have been revised to be consistent with their usage in other methods, and in accordance with the requirements of draft-ietf-sip-message-07.
Consequences if not approved:	⌘	Inconsistent profile specification

Clauses affected:	⌘	A.2.1.2, A.2.1.4.7A, A.2.2.2, A.2.2.3, A.2.2.4.7A (new)

Y	N

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

How to create CRs using this form:

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

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

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

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

FIRST PROPOSED CHANGE

A.1.3 Roles

Table A.2: Roles

Item	Roles	Reference	RFC status	Profile status
1	User agent		o.1	o.1
2	Proxy		o.1	o.1
o.1:	It is mandatory to support exactly one of these items.			
NOTE:	For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.			

Table A.3: Roles specific to this profile

Item	Roles	Reference	RFC status	Profile status
1	UE		n/a	o.1
2	P-CSCF		n/a	o.1
3	I-CSCF		n/a	o.1
4	S-CSCF		n/a	o.1
5	BGCF		n/a	o.1
6	MGCF		n/a	o.1
7	AS		n/a	o.1
7A	AS acting as terminating UA, or redirect server		n/a	c2
7B	AS acting as originating UA		n/a	c2
7C	AS acting as a SIP proxy		n/a	c2
7D	AS performing 3rd party call control		n/a	c2
8	MRFC		n/a	o.1
c2:	IF A.3/7 THEN o.2 ELSE n/a - - AS			
o.1:	It is mandatory to support exactly one of these items.			
o.2:	It is mandatory to support at least one of these items.			
NOTE:	For the purposes of the present document it has been chosen to keep the specification simple by the tables specifying only one role at a time. This does not preclude implementations providing two roles, but an entirely separate assessment of the tables shall be made for each role.			

SECOND PROPOSED CHANGE

A.2.1.2 Major capabilities

Table A.4: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
1	client behaviour for registration?	[26] subclause 10.2	m	c3
2	registrar?	[26] subclause 10.3	o	c4
3	client behaviour for session requests?	[26] subclause 13.2	m	o
4	server behaviour for session requests?	[26] subclause 13.3	m	o
5	session release?	[26] subclause 15.1	m	c1
6	timestamping of requests?	[26] subclause 8.2.6.1	o	o
7	authentication between UA and UA?	[26] subclause 22.2	o	o
8	authentication between UA and registrar?	[26] subclause 22.2	o	n/a
9	server handling of merged requests due to forking	[26] 8.2.2.2	m	m
10	client handling of multiple responses due to forking	[26] 13.2.2.4	m	m
11	insertion of date in requests and responses?	[26] subclause 20.17	o	o
12	downloading of alerting information?	[26] subclause 20.4	o	o
	Extensions			
13	The SIP INFO method?	[25]	o	n/a
14	Reliability of provisional responses in SIP?	[27]	o	m
15	the REFER method?	[36]	o	o
16	Integration of resource management and SIP?	[30]	o	m
17	the SIP UPDATE method	[29]	c5	m
18	SIP extensions for caller identity and privacy?	[34]	o	m
19	SIP extensions for media authorization?	[31]	o	m
20	SIP specific event notification	[28]	o	o
21	the use of NOTIFY to establish a dialog	[28] 4.2	o	n/a
22	acting as the notifier of event information	[28]	c2	c2
23	acting as the recipient of event information	[28]	c2	c2
24	Path Extension Header for Establishing Service Route with SIP REGISTER	[35]	o	c6
25	extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks	[34]	o	m
26	a Privacy Mechanism for the Session Initiation Protocol (SIP)	[33]	o	m
27	a~~A~~ messaging mechanism for the Session Initiation Protocol (SIP)	[50]	o	c7~~m~~

c1: IF A.4/3 OR A.4/4 THEN m ELSE o.
c2: IF A.4/20 THEN o.1 ELSE n/a.
c3: IF A.3/1 OR A.3/4 THEN m ELSE n/a - - UA or S-CSCF functional entity.
c4: IF A.3/4 OR A.3/7 THEN m ELSE n/a - - S-CSCF or AS functional entity.
c5: IF A.4/16 THEN m ELSE o - - integration of resource management and SIP.
c6: IF (A.150/3 AND A.150/4) THEN m ELSE n/a. - - S-CSCF acting as registrar.
c7: IF A.3/1 OR A.3/7B OR A.3/7D THEN m ELSE n/a - - UE or AS acting as originating UA, or AS performing 3rd party call control
o.1: At least one of these capabilities is supported.

FOR INFORMATION, NO CHANGE PROVIDED

A.2.1.3 PDUs

Table A.5: Supported methods

Item	PDU	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	ACK request	[26] 13	m	m	[26] 13	m	m
2	BYE request	[26] 15.1	o		[26] 15.1	o	
3	BYE response	[26] 15.1	o		[26] 15.1	o	
4	CANCEL request	[26] 9	o		[26] 9	o	
5	CANCEL response	[26] 9	o		[26] 9	o	
6	INFO request	[25] 2	c2	n/a	[25] 2	c2	n/a
7	INFO response	[25] 2	c2	n/a	[25] 2	c2	n/a
8	INVITE request	[26] 13	m	m	[26] 13	m	m
9	INVITE response	[26] 13	m	m	[26] 13	m	m
9A	MESSAGE request	[50] 4	c7	c7	[50] 7	c7	c7
9B	MESSAGE response	[50] 4	c7	c7	[50] 7	c7	c7
10	NOTIFY request	[28] 8.1.2	c4	c4	[28] 8.1.2	c3	c3
11	NOTIFY response	[28] 8.1.2	c3	c3	[28] 8.1.2	c4	c4
12	OPTIONS request	[26] 11	m	m	[26] 11	m	m
13	OPTIONS response	[26] 11	m	m	[26] 11	m	m
14	PRACK request	[27] 6	c5	c5	[27] 6	c5	c5
15	PRACK response	[27] 6	c5	c5	[27] 6	c5	c5
16	REFER request	[36] 3	c1	c1	[36] 3	c1	c1
17	REFER response	[36] 3	c1	c1	[36] 3	c1	c1
18	REGISTER request	[26] 10	o		[26] 10	n/a	
19	REGISTER response	[26] 10	n/a		[26] 10	m	
20	SUBSCRIBE request	[28] 8.1.1	c3	c3	[28] 8.1.1	c4	c4
21	SUBSCRIBE response	[28] 8.1.1	c4	c4	[28] 8.1.1	c3	c3
22	UPDATE request	[30] 6.1	c6	c6	[30] 6.2	c6	c6
23	UPDATE response	[30] 6.2	c6	c6	[30] 6.1	c6	c6
c1:	IF A.4/15 THEN m ELSE n/a.						
c2:	IF A.4/13 THEN m ELSE n/a.						
c3:	IF A.4/23 THEN m ELSE n/a.						
c4:	IF A.4/22 THEN m ELSE n/a.						
c5:	IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses.						
c6:	IF A.4/17 THEN m ELSE n/a - - the SIP update method.						
c7:	IF A.4/27 THEN m ELSE n/a - - the SIP MESSAGE method.						

Editor's note: Optional status of BYE in RFC status is given because RFC states SHOULD (client and server).

Editor's note: Optional status of REGISTER in RFC status is given because RFC states RECOMMENDED (client); for the UAS, not statement is made, but it is assumed that this therefore means n/a.

THIRD PROPOSED CHANGE

A.2.1.4.7A MESSAGE method

Prerequisite A.5/9A - - MESSAGE request

Table A.62A: Supported headers within the MESSAGE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[50] 10	m		[50] 10	m	
2	Accept-Encoding	[50] 10	m		[50] 10	m	
3	Accept-Language	[50] 10	m		[50] 10	m	
4	Alert-Info	[50] 10	-		[50] 10	-	
15	Allow	[5026] 1020.5	o	o	[2650] 1020.5	m	m
26	Allow-Events	[2850] 8.2.210	n/ac1	c1	[5028] 108.2.2	n/ac2	c2
7	Anonymity	[50] 10	n/a		[50] 10	n/a	
xxx	Authentication-Info	[50] 10	o		[50] 10	o	
38	Authorization	[5026] 20.710	oc3	c3	[5026] 1020.7	oc3	c3
49	Call-ID	[5026] 1020.8	m	m	[5026] 1020.8	m	m
510	Call-Info	[5026] 1029.9	o	o	[5026] 1029,9	o	o
11	Contact	[50] 10	o		[50] 10	o	
612	Content-Disposition	[5026] 1020.11	o	o	[5026] 1020.11	om	m
713	Content-Encoding	[5026] 1020.12	o	o	[5026] 1012	om	m
814	Content-Language	[5026] 1013	o	o	[5026] 1013	om	m
915	Content-Length	[5026] 1014	tm	m	[5026] 1014	tm	m
1016	Content-Type	[5026] 1015	*m	m	[5026] 1015	*m	m
1117	Cseq	[5026] 1020.16	m	m	[5026] 1020.16	m	m
1218	Date	[5026] 1020.17	oc4	c4	[5026] 1020.17	om	m
1319	Expires	[2650] 20.1910	o	o	[5026] 1020.19	o	o
Xxx	Error-Info	[50] 10	o		[50] 10	o	
xxx	Expires	[50] 10	o		[50] 10	o	
1420	From	[2650] 1020.20	m	m	[5026] 1020.20	m	m
1521	In-Reply-To	[5026] 1020.21	o	o	[5026] 1020.21	o	o
1622	Max-Forwards	[5026] 1022	mo	o	[5026] 1022	mn/a	n/a
1723	MIME-Version	[5026] 2410	-o	o	[50] 10	-m	m
1824	Organization	[5026] 1020.25	o	o	[2650] 20.2510	o	o
25	P-Media-Authorization	[50] 10	n/a		[50] 10	n/a	
1926	Priority	[5026] 1020.26	o	o	[5026] 1020.26	o	o
2027	Proxy-Authorization	[5026] 20.2810	oc5	c5	[50] 10	on/a	n/a
2128	Proxy-Require	[5026] 20.2910	c6o	c6	[5026] 1020.29	on/a	n/a
2229	Record-Route	[5026] 1020.30	-n/a	n/a	[5026] 1020.30	-n/a	n/a

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
30	Remote-Party-ID	[50] 10	n/a		[50] 10	n/a	
2331	Reply-To	[5026] 1020.31	o	o	[5026] 1020.31	o	o
2432	Require	[5026] 1020.32	c8	o	[5026] 1020.32	m	m
xxx	Retry-After	[50] 10	o		[50] 10	o	
2533	Route	[5026] 1020.34	m	m	[5026] 1020.34	n/a	n/a
xxx	Server	[50] 10	o		[50] 10	o	
2634	Subject	[26] 20.36[50] 10	o	o	[26] 20.36[50] 10	o	o
2735	Supported	[5026] 1020.37	n/ac9	m	[5026] 1020.37	n/am	m
2836	Timestamp	[5026] 1020.38	oc10	c10	[5026] 1020.38	om	m
2937	To	[5026] 1020.39	m	m	[5026] 1020.39	m	m
xxx	Unsupported	[50] 10	o		[50] 10	o	
3038	User-Agent	[5026] 1020.41	o	o	[5026] 1020.41	o	o
3139	Via	[5026] 1020.42	m	m	[5026] 1020.42	m	m
xxx	Warning	[50] 10	m		[50] 10	m	
xxx	WWW-Authenticate	[50] 10	o		[50] 10	o	

c1: IF A.4/20 THEN o ELSE n/a - - SIP specific event notification extension.
c2: IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c3: IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.
c4: IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c5: IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.
c6: IF A.4/18 THEN m ELSE o - - (note)
c8: IF A.4/14 THEN o.1 ELSE o - - Reliable transport.
c9: IF IF A.4/14 THEN o.1 ELSE o - - support of reliable transport.
c10: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.

Prerequisite A.5/9A - - MESSAGE request

Table A.62B: Supported message bodies within the MESSAGE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.5/9B - - MESSAGE response

Table A.62C: Supported headers within the MESSAGE response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
3	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
4	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
5	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
6	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
7	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
8	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
9	Date	[26] 20.17	c1	c1	[26] 20.17	m	m
10	From	[26] 20.20	m	m	[26] 20.20	m	m
11	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
12	Organization	[26] 20.25	o	o	[26] 20.25	o	o
13	Server	[26] 20.35	o	o	[26] 20.35	o	o
14	Timestamp	[26] 20.38	m	m	[26] 20.38	c2	c2
15	To	[26] 20.39	m	m	[26] 20.39	m	m
16	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
17	Via	[26] 20.42	m	m	[26] 20.42	m	m
18	Warning	[26] 20.43	o	o	[26] 20.43	o	o
c1:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.						
c2:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.						
NOTE:	For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/6 - - 2xx

Table A.62D: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[50] 10	m	m
2	Authentication-Info	[26] 20.6	c1	c1	[26] 20.6	c2	c2
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
c1:	IF A.4/7 THEN o ELSE n/a - - authentication between UA and UA.						
c2:	IF A.4/7 THEN m ELSE n/a - - authentication between UA and UA.						

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 OR A.6/35 - - 3xx or 485 (Ambiguous)

Table A.62E: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[50] 10	m	m
2	Contact	[26] 20.10	o (note)	o	[26] 20.10	m	m
3	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
NOTE:	The strength of this requirement is RECOMMENDED rather than OPTIONAL.						

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/14 - - 401 (Unauthorized)

Table A.62F: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[50] 10	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	m	m
c1:	IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/17 OR A.6/23 OR A.6/30 OR A.6/36 OR A.6/42 OR A.6/45 OR A.6/50 OR A.6/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.62G: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[50] 10	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Retry-After	[26] 20.33	o	o	[26] 20.33	o	o
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/18 - - 405 (Method Not Allowed)

Table A.62H: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/20 - - 407 (Proxy Authentication Required)

Table A.62I: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[50] 10	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Proxy-Authenticate	[26] 20.27	c1	c1	[26] 20.27	c1	c1
4	Require	[26] 20.32	m	m	[26] 20.32	m	m
5	Supported	[26] 20.37	m	m	[26] 20.37	m	m
6	WWW-Authenticate	[26] 20.44	o	o	[26] 20.44	o	o
c1:	IF A.5/7 THEN m ELSE n/a - - support of authentication between UA and UA.						

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/25 - - 415 (Unsupported Media Type)

Table A.62J: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o.1	o.1	[26] 20.1	m	m
2	Accept-Encoding	[26] 20.2	o.1	o.1	[26] 20.2	m	m
3	Accept-Language	[26] 20.3	o.1	o.1	[26] 20.3	m	m
4	Allow	[26] 20.5	o	o	[50] 10	m	m
5	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
6	Require	[26] 20.32	m	m	[26] 20.32	m	m
7	Supported	[26] 20.37	m	m	[26] 20.37	m	m
o.1	At least one of these capabilities is supported.						

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/27 - - 420 (Bad Extension)

Table A.62K: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[50] 10	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m
5	Unsupported	[26] 20.40	m	m	[26] 20.40	m	m

Prerequisite A.5/9B - - MESSAGE response

Prerequisite: A.6/34 - - 484 (Address Incomplete)

Table A.62L: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	o	o	[50] 10	m	m
2	Error-Info	[26] 20.18	o	o	[26] 20.18	o	o
3	Require	[26] 20.32	m	m	[26] 20.32	m	m
4	Supported	[26] 20.37	m	m	[26] 20.37	m	m

Prerequisite A.5/9B - - MESSAGE response

Table A.62M: Supported message bodies within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

FOURTH PROPOSED CHANGE

A.2.2.2 Major capabilities

Table A.162: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
1	client behaviour for session requests?	[26] 16	m	m
2	server behaviour for session requests?	[26] 16	m	m
3	session release?	[26] 16	m	m
4	Stateless proxy behaviour?	[26] 16.11	o.1	
5	Stateful proxy behaviour?	[26] 16.2	o.1	
6	forking of initial requests	[26] 16.1	c1	n/a
7	support of TLS connections on the upstream side	[26] 16.7	o	n/a
8	support of TLS connections on the downstream side	[26] 16.7	o	n/a
9	insertion of date in requests and responses	[26] 20.17	o	o
10	suppression or modification of alerting information data	[26] 20.4	o	o
11	reading the contents of the Require header before proxying the request or response	[26] 20.32	o	o
12	adding or modifying the contents of the Require header before proxying the REGISTER request or response	[26] 20.32	o	m
13	adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER	[26] 20.32	o	o
14	the requirement to be able to insert itself in the subsequent transactions in a dialog	[26] 16.6	o	c2
15	the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing	[26] 16.7	c3	c3
16	reading the contents of the Supported header before proxying the response	[26] 20.37	o	o
17	reading the contents of the Unsupported header before proxying the 420 response to a REGISTER	[26] 20.40	o	m
18	reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER	[26] 20.40	o	o
19	the inclusion of the Error-Info header in 3xx - 6xx responses	[26] 20.18	o	o
	Extensions			
20	The SIP INFO method?	[25]	o	o
21	Reliability of provisional responses in SIP?	[27]	o	m
22	the REFER method?	[36]	o	o
23	Integration of resource management and SIP?	[30]	o	m
24	the SIP UPDATE method	[29]	c4	m
25	SIP extensions for caller identity and privacy?	[34]	o	m
26	SIP extensions for media authorization?	[31]	o	m
27	SIP specific event notification	[28]	o	o
28	the use of NOTIFY to establish a dialog	[28] 4.2	o	n/a
29	Path Extension Header for Establishing Service Route with SIP REGISTER	[35]	o	c5

30	extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks	[34]	o	m
31	a Privacy Mechanism for the Session Initiation Protocol (SIP)	[33]	o	m
32	a messaging mechanism for the Session Initiation Protocol (SIP)	[50]	o	m
c1:	IF A.162/5 THEN o ELSE n/a			
c2:	IF A.3/4 OR A.3/7 THEN m ELSE IF A.3/3 THEN o ELSE n/a - - S-CSCF or AS else I-CSCF			
c3:	IF (A.162/7 AND NOT A.162/8) OR (NOT A.162/7 AND A.162/8) THEN m ELSE IF A.162/14 THEN o ELSE n/a - - TLS interworking with non-TLS else proxy insertion			
c4:	IF A.162/23 THEN m ELSE o - - integration of resource management and SIP			
c5:	IF A.3/2 OR A.3/3 THEN m ELSE n/a. - - P-CSCF or I-CSCF.			
o.1:	It is mandatory to support at least one of these items.			

FIFTH PROPOSED CHANGE

A.2.2.3 PDUs

Table A.163: Supported methods

Item	PDU	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	ACK request	[26] 13	m	m	[26] 13	m	m
2	BYE request	[26] 16	o	m	[26] 16	o	m
3	BYE response	[26] 16	o	m	[26] 16	o	m
4	CANCEL request	[26] 16.10	o	m	[26] 16.10	o	m
5	CANCEL response	[26] 16.10	o	m	[26] 16.10	o	m
6	INFO request	[25] 2	c2	c2	[25] 2	c2	c2
7	INFO response	[25] 2	c2	c2	[25] 2	c2	c2
8	INVITE request	[26] 16	m	m	[26] 16	m	m
9	INVITE response	[26] 16	m	m	[26] 16	m	m
9A	MESSAGE request	[50] 4	c5	c5	[50] 7	c5	c5
9B	MESSAGE response	[50] 4	c5	c5	[50] 7	c5	c5
10	NOTIFY request	[28] 8.1.2	c3	c3	[28] 8.1.2	c3	c3
11	NOTIFY response	[28] 8.1.2	c3	c3	[28] 8.1.2	c3	c3
12	OPTIONS request	[26] 16	m	m	[26] 16	m	m
13	OPTIONS response	[26] 16	m	m	[26] 16	m	m
14	PRACK request	[27] 6	m	m	[27] 6	m	m
15	PRACK response	[27] 6	m	m	[27] 6	m	m
16	REFER request	[36] 3	c1	c1	[36] 3	c1	c1
17	REFER response	[36] 3	c1	c1	[36] 3	c1	c1
18	REGISTER request	[26] 16	m	m	[26] 16	m	m
19	REGISTER response	[26] 16	m	m	[26] 16	m	m
20	SUBSCRIBE request	[28] 8.1.1	c3	c3	[28] 8.1.1	c3	c3
21	SUBSCRIBE response	[28] 8.1.1	c3	c3	[28] 8.1.1	c3	c3
22	UPDATE request	[30] 7	c4	c4	[30] 7	c4	c4
23	UPDATE response	[30] 7	c4	c4	[30] 7	c4	c4
c1:	IF A.162/22 THEN m ELSE n/a.						
c2:	IF A.162/20 THEN m ELSE n/a.						
c3	IF A.162/27 THEN m ELSE n/a.						
c4	IF A.162/24 THEN m ELSE n/a - - the SIP UPDATE method.						
c5:	IF A.162/32 THEN m ELSE n/a - - the SIP MESSAGE method.						

SIXTH PROPOSED CHANGE - NEW CLAUSE

A.2.2.4.7A MESSAGE method

Prerequisite A.163/9A - - MESSAGE request

Table A.218A: Supported headers within the MESSAGE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	i	i
2	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
3	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
4	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
5	Call-Info	[26] 20.9	m	m	[26] 20.9	c4	c4
6	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
7	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
8	Content-Language	[26] 20.13	m	m	[26] 20.13	i	i
9	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
10	Content-Type	[26] 20.15	m	m	[26] 20.15	i	i
11	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
12	Date	[26] 20.17	m	m	[26] 20.17	c2	c2
13	Expires	[26] 20.19	m	m	[26] 20.19	I	i
14	From	[26] 20.20	m	m	[26] 20.20	m	m
15	In-Reply-To	[26] 20.21	m	m	[50] 10	i	i
16	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
17	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
18	Organization	[26] 20.25	m	m	[26] 20.25	c3	c3
19	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	c8	c8
20	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
21	Record-Route	[26] 20.30	m	m	[26] 20.30	c7	c7
22	Require	[26] 20.32	m	m	[26] 20.32	c5	c5
23	Route	[26] 20.34	m	m	[26] 20.34	m	m
24	Subject	[26] 20.36	m	m	[26] 20.36	i	i
25	Supported	[26] 20.37	m	m	[26] 20.37	c6	c6
26	Timestamp	[26] 20.38	m	m	[26] 20.38	i	i
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
29	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1: IF A.4/20 THEN m ELSE i - - SIP specific event notification extension.
c2: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.
c3: IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.
c4: IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.
c5: IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.
c6: IF A.162/16 THEN m ELSE i - - reading the contents of the Supported header before proxying the response.
c7: IF A.162/14 THEN o ELSE i - - the requirement to be able to insert itself in the subsequent transactions in a dialog.
c8: IF A.162/8A THEN m ELSE i - - authentication between UA and proxy.

NOTE: c1 refers to the UA role major capability as this is the case of a proxy that also acts as a UA specifically for SUBSCRIBE and NOTIFY.

Prerequisite A.163/9A - - MESSAGE request

Table A.218B: Supported message bodies within the MESSAGE request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							

Prerequisite A.163/9B - - MESSAGE response

Table A.218C: Supported headers within the MESSAGE response - all remaining status-codes

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
2	Call-Info	[26] 20.9	m	m	[26] 20.9	c3	c3
3	Content-Disposition	[26] 20.11	m	m	[26] 20.11	i	i
4	Content-Encoding	[26] 20.12	m	m	[26] 20.12	i	i
5	Content-Language	[26] 20.13	m	m	[26] 20.13	i	i
6	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
7	Content-Type	[26] 20.15	m	m	[26] 20.15	i	i
8	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
9	Date	[26] 20.17	m	m	[26] 20.17	c1	c1
10	From	[26] 20.20	m	m	[26] 20.20	m	m
11	MIME-Version	[26] 20.24	m	m	[26] 20.24	i	i
12	Organization	[26] 20.25	m	m	[26] 20.25	c2	c2
13	Server	[26] 20.35	m	m	[26] 20.35	i	i
14	Timestamp	[26] 20.38	i	i	[26] 20.38	i	i
15	To	[26] 20.39	m	m	[26] 20.39	m	m
16	User-Agent	[26] 20.41	m	m	[26] 20.41	i	i
17	Via	[26] 20.42	m	m	[26] 20.42	m	m
18	Warning	[26] 20.43	m	m	[26] 20.43	i	i
c1:	IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.						
c2:	IF A.162/19A OR A.162/19B THEN m ELSE i - - reading, adding or concatenating the Organization header.						
c3:	IF A.162/19C OR A.162/19D THEN m ELSE i - - reading, adding or concatenating the Call-Info header.						

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/6 - - 2xx

Table A.218D: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Authentication-Info	[26] 20.6	m	m	[26] 20.6	i	i
3	From	[26] 20.20	m	m	[26] 20.20	m	m
4	Record-Route	[26] 20.30	m	m	[26] 20.30	c3	c3
5	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
6	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.						
c3:	IF A.162/15 THEN o ELSE i - - the requirement to be able to use separate URIs in the upstream direction and downstream direction when record routeing.						

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 OR A.164/35 - - 3xx or 485 (Ambiguous)

Table A.218E: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	i	i
2	Contact	[26] 20.10	m	m	[26] 20.10	c1	c1
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c1:	IF A.162/19E THEN m ELSE i - - deleting Contact headers.						
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.						

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/14 - - 401 (Unauthorized)

Table A.218F: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
4	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.						

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/17 OR A.164/23 OR A.164/30 OR A.164/36 OR A.164/42 OR A.164/45 OR A.164/50 OR A.164/51 - - 404, 413, 480, 486, 500, 503, 600, 603

Table A.218G: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Retry-After	[26] 20.33	m	m	[26] 20.33	i	i
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.						

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/18 - - 405 (Method Not Allowed)

Table A.218H: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[26] 20.5	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.						

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/20 - - 407 (Proxy Authentication Required)

Table A.218I: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Proxy-Authenticate	[26] 20.27	m	m	[26] 20.27	m	m
4	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
6	WWW-Authenticate	[26] 20.44	m	m	[26] 20.44	i	i
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.						

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/25 - - 415 (Unsupported Media Type)

Table A.218J: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	m	m	[26] 20.1	i	i
2	Accept-Encoding	[26] 20.2	m	m	[26] 20.2	i	i
3	Accept-Language	[26] 20.3	m	m	[26] 20.3	i	i
4	Allow	[26] 20.5	m	m	[50] 10	i	i
5	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
6	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
7	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.						

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/27 - - 420 (Bad Extension)

Table A.218K: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	i	i
2	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
3	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
4	Supported	[26] 20.37	m	m	[26] 20.37	i	i
5	Unsupported	[26] 20.40	m	m	[26] 20.40	c3	c3
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.						
c3:	IF A.162/18 THEN m ELSE i - - reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER.						

Prerequisite A.163/9B - - MESSAGE response

Prerequisite: A.164/34 - - 484 (Address Incomplete)

Table A.218L: Supported headers within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Allow	[26] 20.5	m	m	[50] 10	i	i
2	Contact	[26] 20.10	o		[26] 20.10	o	
3	Error-Info	[26] 20.18	m	m	[26] 20.18	i	i
4	Require	[26] 20.32	m	m	[26] 20.32	c2	c2
5	Supported	[26] 20.37	m	m	[26] 20.37	i	i
c2:	IF A.162/11 OR A.162/13 THEN m ELSE i - - reading the contents of the Require header before proxying the request or response or adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER.						

Prerequisite A.163/9B - - MESSAGE response

Table A.218M: Supported message bodies within the MESSAGE response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1							