3GPP TSG CN Plenary Meeting #18 **NP-020566**
4th - 6th December 2002. New Orleans, USA.

Source: **TSG CN WG 1**

Title: **CR to Rel-5 on Work Item IMS-CCR towards 24.229,- CR278r3**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **1** CR, **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	278	3	F	Rel-5	P-CSCF does not strip away headers	N1-27	N1-022499	5.2.0

First proposed change

5 Application usage of SIP

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].

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 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 include a Supported header containing the option tag "path".

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. In order to build a proper preloaded Route header value for new dialogs, the UE shall also store the list of Service Route headers contained in the Service-Route header.

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

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

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

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

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

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

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

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

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

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

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

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

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

The UE shall include a Supported header containing the option tag "path".

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, 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. The Call-ID of the integrity protected REGISTER request which carries RES must be the same as the Call-ID of the 401 which carried the challenge.

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

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

The request shall be sent integrity protected.

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

5.1.1.7 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.

5.1.2 Subscription and notification

5.1.2.1 Notification about multiple registered public user identities

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

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

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

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

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

5.1.2.2 General SUBSCRIBE requirements

If the UA receives a 503 (Service Unavailable) response to an initial SUBSCRIBE 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.

5.1.2A Generic procedures applicable to all methods

5.1.2A.1 Mobile-originating case

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

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

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

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

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

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

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

The UE shall build a proper preloaded Route header value for all new dialogs and standalone transactions. The UE shall build a list of Route header values made out of, in this order, the P-CSCF URI (learnt through the P-CSCF discovery procedures) and the values received in the Service-Route header saved from the 200 (OK) response to the last registration or re-registration.

5.1.2A.2 Mobile-terminating case

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

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

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

5.1.3 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~~ validate the routeing information in~~to~~ 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~~ list 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;~~

3~~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;

4~~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.

5~~6~~) store the values received in the P-Charging-Function-Addresses header; and

6~~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 header lists. The first Route header list - created during the registration procedure ~~-~~ is used only to ~~pre-load~~validate the routeing information in~~to~~ the initial ~~INVITE~~ requests that originat~~ed~~ from~~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-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~~

1) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) is matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCFshall either:

    a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or

    b) replace the preloaded Route header value in the request with the value of the Service-Route header received during the last 200 (OK) response for a registration or reregistration;

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

2~~4~~) ~~create~~ add its own SIP URI to the top of the ~~a~~ Record-Route header ~~containing its own SIP URL~~ The P-CSCF SIP URI is built in a format that contains the port number of the security association established from the UE to the P-CSCF and either:~~;~~

    a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

    b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

3~~5~~) insert a P-Asserted-Identity header with a value representing the initiator of the request;

~~6~~4) create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and

~~7~~5) 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~~ store 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~~3) store the dialog ID and associate it with the private user identity and public user identity involved in the session;

~~5~~4) save the Contact header received in the response in order to release the dialog if needed; and

~~6~~5) 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) verify that the list of Route headers in the request is included, preserving the same order, in the list of Record-Route headers that was received during the last target refresh request for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

    a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

    b) replace the Route header value in the request with the one received during the last target refresh request for the same dialog in the Record-Route header.

~~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~~3) ~~create~~ add its own SIP URI to the~~a~~ Record-Route header. ~~containing its own SIP URL~~The P-CSCF SIP URI is built in a format that contains the port number of the security association established from the UE to the P-CSCF and either:

a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

b) the P-CSCF IP address of the security association established from the UE to the P-CSCF; and

~~6~~4) 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~~ store 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~~2) save the Contact header received in the response in order to release the dialog if needed; and

~~4~~3) 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) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) matches the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCFshall either:

a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

~~remove any Route header from the request;~~

b) replace the preloaded Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response.~~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~~2) insert a P-Asserted-Identity header with a value representing the initiator of the request;

~~5~~3) create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and

~~6~~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) 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) verify that the list of Route headers in the request matches the list of Record-Route headers that was received during the last target refresh request for the same dialog. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 3 onwards; or

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

   b) replace the Route header value in the request with the one received during the last target refresh request for the same dialog in the Record-Route header.

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

~~4~~3) 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~~

~~1~~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) verify that the list of URIs received in the Service-Route header (during the last successful registration or re-registration) is included, preserving the same order, as a subset of the preloaded Route headers in the received request. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCFshall either:

   a) return a 400 (Bad Request) response that may include a Warning header containing the warn-code 399; the P-CSCF shall not forward the request, and shall not continue with the execution of steps 2 onwards; or

   ~~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;~~

   b) replace the Route header value in the request with the one received during the last registration in the Service-Route header of the 200 (OK) response.~~2) pre-load the list of Route headers to the request,~~

~~3~~2) insert an P-Asserted-Identity header with a value representing the initiator of the request; and

~~4~~3) 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~~1) 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) save the Record-Route header list;

~~2~~3) ~~remove the list of Record-Route headers, and shall~~ convert ~~it~~ the list of Record-Route header values into a list of Route header~~s~~ values, and ~~. 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~~;

4~~3~~) save the Contact header received in the ~~response~~ request in order to release the dialog if needed;

5~~4~~) add its own SIP URI ~~itself on~~ to 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~~;The P-CSCF SIP URI is built in a format that contains the port number of the security association established from the UE to the P-CSCF and either:

a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

6~~5~~) ~~remove and~~ add its own address to the top of the received list of Via header and save the list; ~~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;~~ The P-CSCF Via header entry is built in a format that contains the port number of the security association established from the UE to the P-CSCF and either:

a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

7~~6~~) store the values received in the P-Charging-Function-Addresses header; and

8~~7~~) remove and store the icid parameter received in the P-Charging-Vector header.

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

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

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

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

2) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

a) discard the response; or

b) replace the Via header values with those received in the request;

3) verify that the list of URIs received in the Record-Route header of the request corresponding to the same dialog is included, preserving the same order, as a subset of the Record-Route header list of this response. This verification is done on a per URI basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

a) discard the response; or

b) replace the Via header values with those received in the request;

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) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

a) discard the response; or

b) replace the Via header values with those received in the request;

~~1~~2) forward the response based on the~~append the saved~~ list of Via headers in~~to~~ the response.

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

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

2) save, if present, the received Record-Route headers of the received request;

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

4) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the port number of the security association established from the UE to the P-CSCF and either:

a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

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) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If the verification fails, then the P-CSCF shall either:

a) discard the response; or

b) replace the Via header values with those received in the request;

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) add its own address to the top of the received list of Via header and save the list.~~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;~~ The P-CSCF Via header entry is built in a format that contains the port number of the security association established from the UE to the P-CSCF and either:

a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

b) the P-CSCF IP address of the security association established from the UE to the P-CSCF;

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

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

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

1) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

a) discard the response; or

b) replace the Via header values with those received in the request;

~~1~~2) forward the response based on the ~~append the saved~~ list of Via headers in~~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) add its own address to the top of the received list of Via header and save the list~~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~~ The P-CSCF Via header entry is built in a format that contains the port number of the security association established from the UE to the P-CSCF and either:

a) the P-CSCF FQDN that resolves to the IP address of the security association established from the UE to the P-CSCF; or

b) the P-CSCF IP address of the security association established from the UE to the P-CSCF; 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) verify that the list of Via headers matches the saved list of Via headers received in the request corresponding to the same dialog, including the P-CSCF via header value. This verification is done on a per Via header value basis, not as a whole string. If these lists do not match, then the P-CSCF shall either:

a) discard the response; or

b) replace the Via header values with those received in the request;

~~1~~2) forward the response based on the ~~append the saved~~ list of Via headers ~~to~~ in the response.

5.2.7 Initial INVITE

5.2.7.1 Introduction

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

5.2.7.2 Mobile-originating case

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

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

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

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

5.2.7.3 Mobile-terminating case

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

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

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

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

5.2.7.4 GPRS charging information

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

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

5.2.8 Call release

5.2.8.1 P-CSCF-initiated call release

5.2.8.1.1 Cancellation of a session currently being established

Upon receipt of an indication that radio coverage is no longer available for a served user, for whom one ore more ongoing multimedia session are currently being established, the P-CSCF shall cancel the related dialogs by sending out a CANCEL request according to the procedures described in RFC 3261 [26].

5.2.8.1.2 Release of an existing session

Upon receipt of an indication that the radio interface resources are no longer available for a served user, for whom one or more ongoing session exists, the P-CSCF shall release each of the related dialogs by applying the following steps:

1) if the P-CSCF serves the calling user of a session it shall generate a BYE request based on the information saved for the related dialog, including:

    - a Request-URI, set to the stored Contact header provided by the called user;

    - a To header, set to the To header value as received in the 200 (OK) response for the initial INVITE request;

    - a From header, set to the From header value as received in the initial INVITE request;

- a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
- a CSeq header, set to the CSeq value that was stored for the direction from the calling to the called user, incremented by one;
- a Route header, set to the routeing information towards the called user as stored for the dialog;
- further headers, based on local policy or the requested session release reason.

2) If the P-CSCF serves the called user of a session it shall generate a BYE request based on the information saved for the related dialog, including:

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

3) send the so generated BYE request towards the indicated user.

4) upon receipt of the 2xx responses for the BYE request, shall delete all information related to the dialog and the related multimedia session.

5.2.8.1.3 Abnormal cases

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

5.2.8.2 Call release initiated by any other entity

When the P-CSCF receives a 2xx response for a BYE request matching an existing dialog, it shall delete all the stored information related to the dialog.

5.2.9 Subsequent requests

5.2.9.1 Mobile-originating case

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

5.2.9.2 Mobile-terminating case

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

5.2.10 Emergency service

The P-CSCF shall inspect the Request URI of all INVITE requests for known emergency numbers and emergency URLs from a configurable list. If the P-CSCF detects that the Request-URI of the INVITE request matches one of the numbers in this list, the INVITE request shall not be forwarded. The P-CSCF shall answer the INVITE request with a 380 (Alternative Service) response.

The 380 (Alternative Service) response shall contain a Content-Type header field with the value set to associated MIME type of the 3GPP IMS XML body as described in subclause 7.6.1.

The 3GPP IMS XML body shall contain an <alternative-service> element that indicates the parameters of the alternative service. The <type> child element shall be set to "emergency" to indicate that it was an emergency call. An operator configurable <reason> child element shall be included with a reason phrase.

The P-CSCF shall have a configurable list of emergency numbers and emergency URLs (e.g. sos@domain). The list is used to determine whether the INVITE is destined for an emergency centre or not.

5.2.11 MESSAGE support

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

Next 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
3A	I-CSCF (THIG)		n/a	c1
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
8	MRFC		n/a	o.1
c1: IF A.3/3 THEN o ELSE x 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.				

Next proposed change

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

A.2.1 User agent role

A.2.1.1 Introduction

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

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

A.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~~ Session Initiation Protocol Extension Header Field for ~~Establishing Service Route with SIP REGISTER~~Registering Non-Adjacent Contacts	[35]	o	c6
25	extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks	[34]	o	m
26	a Privacy Mechanism for the Session Initiation Protocol (SIP)	[33]	o	m
27	A messaging mechanism for the Session Initiation Protocol (SIP)	[50]	o	m
28	Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration	[38]	o	m
c1:	IF A.4/3 OR A.4/4 THEN m ELSE o.			
c2:	IF A.4/20 THEN o.1 ELSE n/a.			
c3:	IF A.3/1 OR A.3/4 THEN m ELSE n/a - - UA or S-CSCF functional entity.			
c4:	IF A.3/4 OR A.3/7 THEN m ELSE n/a - - S-CSCF or AS functional entity.			
c5:	IF A.4/16 THEN m ELSE o - - integration of resource management and SIP.			
c6:	IF (~~A.150/3 AND A.150/4~~A.3/4) OR A.3/1 THEN m ELSE n/a. - - S-CSCF ~~acting as registrar~~ or UE.			
o.1:	At least one of these capabilities is supported.			

Next proposed change

A.2.1.4.12 REGISTER method

Prerequisite A.5/18 - - REGISTER request

Table A.119: Supported headers within the REGISTER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	c1	c1	[28] 8.2.2	c1	c1
5	Authorization	[26] 20.7	c2	n/a	[26] 20.7	c2	n/a
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	o		[26] 20.9	o	
8	Contact	[26] 20.10	m		[26] 20.10	m	
9	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
10	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
11	Content-Language	[26] 20.13	o		[26] 20.13	o	
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
14	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	c3	c3	[26] 20.17	m	m
16	Expires	[26] 20.19	o		[26] 20.19	o	
17	From	[26] 20.20	m	m	[26] 20.20	m	m
18	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
19	MIME-Version	[26] 20.24	o		[26] 20.24	o	
20	Organization	[26] 20.25	o		[26] 20.25	o	
20A	Path	[35] 4	c4	c5	[35] 4	m	c6
21	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
22	Proxy-Require	[26] 20.29	o	o (note)	[26] 20.29	n/a	n/a
23	Require	[26] 20.32	o	o	[26] 20.32	m	m
24	Route	[26] 20.34	o	n/a	[26] 20.34	n/a	n/a
25	Supported	[26] 20.37	o	o	[26] 20.37	m	m
26	Timestamp	[26] 20.38	m	m	[26] 20.38	c7	c7
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	o		[26] 20.41	o	
29	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1: IF A.4/20 THEN m ELSE n/a.
c2: IF A.4/8 THEN m ELSE n/a.
c3: IF A.4/11 THEN o ELSE n/a.
c4: IF A.4/24 THEN o ELSE n/a
c5: IF A.4/24 THEN x ELSE n/a
c6: IF (A.3/4) OR A.3/1 THEN m ELSE n/a. - - S-CSCF or UE.
c7: IF A.4/6 THEN m ELSE n/a.

NOTE: No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage..

Next proposed change

Table A.123: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	o		[26] 20.5	o	
3	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
4	Call-Info	[26] 20.9	o		[26] 20.9	o	
5	Contact	[26] 20.10	o		[26] 20.10	o	
6	Expires	[26] 20.19	o		[26] 20.19	o	
6A	Path	[35] 4	c3	c3	[35] 4	c4	c4
7	Require	[26] 20.32	m	m	[26] 20.32	m	m
8	Server	[26] 20.35	o	o	[26] 20.35	o	o
8A	Service-Route	[38] 6	c5	c5	[38] 6	c5	c5
9	Supported	[26] 20.37	m	m	[26] 20.37	m	m
10	User-Agent	[26] 20.41	o		[26] 20.41	o	
11	Warning	[26] 20.43	o		[26] 20.43	o	

c1: IF (A.3/4 AND A.4/2) THEN m ELSE n/a. - - S-CSCF acting as registrar.
c2: IF A.3/4 OR A.3/1THEN m ELSE n/a. - - S-CSCF or UE.
c3: IF A.4/24 THEN m ELSE n/a
c4: IF A.4/24 THEN o ELSE n/a
c5: IF A.4/28 THEN m ELSE n/a

Next proposed change

A.2.2 Proxy role

A.2.2.1 Introduction

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

Prerequisite: A.2/2 -- proxy role

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~~ Session Initiation ProtocolExtension Header Field for ~~Establishing Service Route with SIP REGISTER~~ Registering Non-Adjacent Contacts	[35]	o	~~c5~~c6

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	Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration	[38]	o	c6

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.~~

c6: IF A.3/2 OR A.3/3A THEN m ELSE n/a -- P-CSCF or I-CSCF (THIG)

o.1: It is mandatory to support at least one of these items.

Next proposed change

A.2.2.4.12 REGISTER method

Prerequisite A.163/18 – REGISTER request

Table A.275: Supported headers within the REGISTER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Accept-Encoding	[26] 20.2	o		[26] 20.2	o	
3	Accept-Language	[26] 20.3	o		[26] 20.3	o	
4	Allow-Events	[28] 8.2.2	m	m	[28] 8.2.2	c1	c1
5	Authorization	[26] 20.7	m	m	[26] 20.7	i	i
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	o		[26] 20.9	o	
8	Contact	[26] 20.10	m		[26] 20.10	m	
9	Content-Disposition	[26] 20.11	o		[26] 20.11	o	
10	Content-Encoding	[26] 20.12	o		[26] 20.12	o	
11	Content-Language	[26] 20.13	o		[26] 20.13	o	
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
14	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	m	m	[26] 20.17	m	m
16	Expires	[26] 20.19	o		[26] 20.19	o	
17	From	[26] 20.20	m	m	[26] 20.20	m	m
18	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
19	MIME-Version	[26] 20.24	o		[26] 20.24	o	
20	Organization	[26] 20.25	o		[26] 20.25	o	
20A	Path	[35] 4.2	c6	c6	[35] 4.2	c6	c6
21	Proxy-Authorization	[26] 20.28	o		[26] 20.28	o	
22	Proxy-Require	[26] 20.29	m	m	[26] 20.29	m	m
23	Require	[26] 20.32	m	m	[26] 20.32	c4	c4
24	Route	[26] 20.34	m	m	[26] 20.34	m	m
25	Supported	[26] 20.37	m	m	[26] 20.37	c5	c5
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	o		[26] 20.41	o	
29	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1: IF A.4/20 THEN m ELSE i.

c4: IF A.162/11 OR A.162/12 THEN m ELSE i.

c5: IF A.162/16 THEN m ELSE i.

c6: IF A.162/29 THEN m ELSE n/a -- PATH header support

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.

Next proposed change

Prerequisite: A.164/6 – 2xx

Table A.279: Supported headers within the REGISTER response

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o		[26] 20.1	o	
2	Allow	[26] 20.5	o		[26] 20.5	o	
3	Authentication-Info	[26] 20.6	o		[26] 20.6	o	
4	Call-Info	[26] 20.9	o		[26] 20.9	o	
5	Contact	[26] 20.10	o		[26] 20.10	o	
6	Expires	[26] 20.19	o		[26] 20.19	o	
6A	Path	[35] 4.2	c3	c3	[35] 4.2	c4	c4
7	Require	[26] 20.32	m	m	[26] 20.32	c1	c1
8	Server	[26] 20.35	m	m	[26] 20.35	i	i
8A	Service-Route	[38] 6	c5	c5	[38] 6	c6	c7
9	Supported	[26] 20.37	m	m	[26] 20.37	i	i
10	User-Agent	[26] 20.41	o		[26] 20.41	o	
11	Warning	[26] 20.43	o		[26] 20.43	o	
c1:	IF A.162/11 OR A.162/12 THEN m ELSE i.						
c2:	IF A.3/2 OR A.3/3A THEN m ELSE n/a -- P-CSCF or I-CSCF (THIG)						
c3:	IF A.162/29 THEN m ELSE n/a -- Path extension support						
c4:	IF A.162/29 THEN i ELSE n/a -- Path extension support						
c5:	IF A.162/32 THEN m ELSE n/a -- Service-Route extension support						
c5:	IF A.162/32 THEN i ELSE n/a -- Service-Route extension support						
c7:	IF A.162/32 THEN (IF A.3/2 THEN m ELSE I) ELSE n/a -- Service-Route extension and P-CSCF						