3GPP TSG CN Plenary Meeting #20 **NP-030277**
4th - 6th June 2003. HÄMEENLINNA, Finland.

Source: **TSG CN WG 1**

Title: **CRs to Rel-5 on Work Item IMS-CCR towards 24.229,- pack 3**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **9** CRs, **Rel-5 to** Work Item **”IMS-CCR”**, that have been agreed by **TSG CN WG1**, and are forwarded to TSG CN Plenary meeting #20 for approval.

Spec	CR	Rev	Cat	Phase	Subject	Version-Current	Version-New	Meeting-2nd-Level	Doc-2nd-Level
24.229	369	3	F	Rel-5	S-CSCF behavior correction to enable call forwarding	5.4.0	5.5.0	N1-30	N1-030931
24.229	370	1	F	Rel-5	SUBSCRIBE request information stored at the P-CSCF and S-CSCF	5.4.0	5.5.0	N1-30	N1-030521
24.229	371	1	F	Rel-5	Profile Tables - Transparency	5.4.0	5.5.0	N1-30	N1-030858
24.229	375	1	F	Rel-5	Profile Tables - Major Capability Corrections	5.4.0	5.5.0	N1-30	N1-030860
24.229	376	2	F	Rel-5	Profile Tables - Deletion of Elements not used in 24.229	5.4.0	5.5.0	N1-30	N1-030921
24.229	377	1	F	Rel-5	Use of the QoS parameter 'signalling information' for a signalling PDP context	5.4.0	5.5.0	N1-30	N1-030840
24.229	378	2	F	Rel-5	Deregistration of a PUID (not the last one)	5.4.0	5.5.0	N1-30	N1-030919
24.229	379	2	F	Rel-5	'Last registered public user identity' terminology change	5.4.0	5.5.0	N1-30	N1-030920
24.229	380	1	F	Rel-5	Check Integrity Protection for P-Access-Network-Info header	5.4.0	5.5.0	N1-30	N1-030881

3GPP TSG-CN1 Meeting #30 Tdoc N1-030931
San Diego, California, USA, 19 – 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘	**24.229**	**CR**	**369**	⌘ **rev**	**3**	⌘	Current version:	**5.4.0** ⌘

*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 behavior correction to enable call forwarding		
Source:	⌘	Nokia		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	12/05/03
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:	⌘	Call forwarding is disabled in Rel-5 by S-CSCF behavior. Currently, the terminating S-CSCF always replaces the Request-URI with Contact address without even checking whether a forwarding application (located in an AS) has modified the Request-URI
Summary of change:	⌘	Additional step is proposed to make a comparison on the incoming Request-URI and the Request-URI after the request has visited all the ASs.
Consequences if not approved:	⌘	Services based on Request-URI modification won't work in Rel-5

Clauses affected:	⌘	5.4.3.3				
		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	23.218
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘	CR 369 rev3 includes agreed text from CR414 rev2				

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.

5.4.3.3 Requests terminated at the served user

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

1) determine whether the request contains a barred public user identity in the Request-URI of the request or not. In case the Request URI contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 404 (Not Found) response. Otherwise, continue with the rest of the steps;

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

3) save the Request-URI from the request;

4~~3~~)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;

54)check whether the initial request matches the next unexecuted initial filter criteria in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5.~~check whether the initial request matches the initial filter criteria based on the public user identity in the Request-URI,~~ If there is a match, then ~~the S-CSCF shall forward this request to that application server,~~ insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

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

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

66~~5~~) insert a P-Charging-Function-Addresses header field (see subclause 7.2.4), if not present, populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

~~6~~7~~7~~) 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;

88~~7~~) store the value of the orig-ioi parameter received in the P-Charging-Vector header, if present. The orig-ioi parameter identifies the sending network of the request message. The orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS;

99~~8) check~~) check whether the Request-URI equals to~~with~~ the saved value of the Request-URI. If there is no match, then:

a) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed; and~~in case of an initial request for a dialog, create a Record-Route header containing its own SIP URI and save the necessary Record-Route header fields and the Contact header field from the request in order to release the dialog when needed; and~~

b) forward the request~~ make a routing decision~~ based on the Request-URI and skip the following steps;

If there is a match, then continue with the further steps;

10~~10~~) in case there are no Route headers in the request, then determine, from the destination public user identity, the list of preloaded routes saved during registration or re-registration, as described in subclause 5.4.1.2. Furthermore, the S-CSCF shall:~~;~~

a~~1~~1~~9~~) build the Route header field with the values determined in the previous step;

b~~1~~2~~0~~) determine, from the destination public user identity, the saved Contact URI~~L~~ where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2;

c~~1~~3~~1~~) build a Request-URI with the contents of the saved Contact URI~~L~~ determined in the previous step;

d~~1~~4~~2~~) insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;

11~~53~~) in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary Record-Route header fields and the Contact header from the request in order to release the dialog when needed; and

12~~64~~) optionally, apply any privacy required by RFC 3323 [33] to the P-Asserted-Identity header; and

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

13~~75~~) forward the request based on the topmost Route header.

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

1) execute the procedures described in the steps 1, 2, 3~~, 3~~ and 44~~3~~ in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction);

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

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

3~~4~~)execute the procedure described in step 5, 6, 7, 8, 9, 11, 12~~4~~5 and 13~~5~~6 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

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

~~5) execute the procedures described in the steps 76, 78, 124, 135, 146 and 157 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).~~

When the S-CSCF receives a response to the initial request for a dialog (whether the user is registered or not), it shall save the necessary Record-Route header fields and the Contact header field from the response in order to release the dialog if needed. In the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URL contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel-URI In case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header.

When the S-CSCF receives the 200 (OK) response for a standalone transaction request, 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 an AS.

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

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

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

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

When the S-CSCF receives a response to the target refresh request for a dialog (whether the user is registered or not), it shall save the necessary Record-Route header fields and the Contact header field from the response in order to release the dialog if needed. In case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header.

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

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

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

3GPP TSG-CN1 Meeting #29 ***Tdoc N1-030521***
Sophia-Antipolis, France, 31 March – 04 April 2003

CR-Form-v7

CHANGE REQUEST

⌘	**24.229**	**CR**	**370**	⌘ **rev**	**1**	⌘ Current version:	**5.4.0** ⌘

*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:	⌘	SUBSCRIBE request information stored at the P-CSCF and S-CSCF		
Source:	⌘	Ericsson		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	03/04/03
Category:	⌘	**F**	***Release:*** ⌘	Rel-5

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

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

Reason for change:	⌘	The current text in 24.229 suggests that, the P-CSCF and S-CSCF need to store some signalling related information in order to be able to release the session. While this is generally applicable to INVITE requests, it is not applicable to any other request apart INVITE (e.g., SUBSCRIBE), nor procedures are provided at the P-CSCF or S-CSCF to dismiss those subscriptions in any case. The specification lacks to mandate the P-CSCF and S-CSCF to store the CSeq header field values both in INVITE requests and responses, in case the session needs to be released.
Summary of change:	⌘	It is clarified that the storage of certain headers (Contact, etc.) are only applicable when the request is an INVITE or in responses to INVITE requests. Clarified that the relevant information to save are Contact, CSeq and Record-Route in INVITE requests and Contact and Record-Route in responses to INVITE requests.
Consequences if not approved:	⌘	Data is stored in the P-CSCF or S-CSCF without any meaning. Not all the data that needs to be used in case of a session release is stored in the P-CSCF and S-CSCF

Clauses affected:	⌘	5.2.6, 5.4.3.2, 5.4.3.3				
		Y	**N**			
Other specs affected:	⌘	X		Other core specifications	⌘	24.228 CR 109
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

First proposed change

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 target refresh request or a stand-alone transaction, the P-CSCF shall:

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

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

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 a 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-Preferred-Identity header that does not match one of the registered public user identities, or does not contain a P-Preferred-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity. If there is more then one default public user identity available, the P-CSCF shall randomly select one of them.

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 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 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;

2) add its own SIP ~~URL~~ URI to the top of the Record-Route header. 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) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with a value representing the initiator of the request; ~~and~~

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

5) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

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

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

4) if the response corresponds to an INVITE request, save the Contact and Record-Route header field values received in the response ~~in order to~~ such that the P-CSCF is able to release the ~~dialog~~ session if needed;

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

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

a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. 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; and

3) add its own SIP ~~URL~~ URI to the Record-Route header. 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-CSCFbefore forwarding the request, based on the topmost Route header, in accordance with the procedures of RFC 3261 [26];~~.~~

and

4) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

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

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

2) if the response corresponds to an INVITE request, save the Contact and Record-Route header field values received in the response ~~in order to~~ such that the P-CSCF is able to release the ~~dialog~~ session if needed;

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 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

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

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

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 target refresh request, the P-CSCF shall:

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

   a) if the request does not relates to an existing dialog in which the originator is involved, then the P-CSCF shall answer the request by sending a 403 (Forbidden) response back to the originator. The response may include a Warning header containing the warn-code 399. 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; and

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

   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;

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 from the UE the request for an unknown method, and a 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-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 2 onwards; or

   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; and

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

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

5.2.6.4 Requests terminated by the UE

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

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

2) save the Record-Route header list;

3) convert the list of Record-Route header values into a list of Route header values and save this list of Route headers;

4) if the request is an INVITE request, save a copy of the Contact, ~~-~~CSeq and Record-Route header field values received in the request~~ in order to~~ such that the P-CSCF is able to release the ~~dialog~~ session if needed;

5) add its own SIP URI to the top of the list of Record-Route headers and save the list. 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) 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;

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

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

9) save a copy of the P-Called-Party-ID 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) remove the P-Preferred-Identity header, if present, and insert a P-Asserted-Identity header with the value saved from the P-Called-Party-ID header that was received in the request;

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; and

5) if the response corresponds to an INVITE request, save the Contact and Record-Route header field value received in the response such that the P-CSCF is able to release the session if needed;

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) 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;

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

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~~ URI 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~~2) 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;

    and

3) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the P-CSCF is able to release the session if needed;

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;

    and

2) if the response corresponds to an INVITE request, save the Contact and Record-Route header field values received in the response such that the P-CSCF is able to release the session if needed;

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) 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;

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

3) 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) 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; and

2) 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;

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 target 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 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;

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 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;

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

Next proposed change

5.4.3.2 Requests initiated by the served user

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

1) determine whether the request contains a barred public user identity in the P-Asserted-Identity or From 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 may include a Warning header containing the warn-code 399. Otherwise, continue with the rest of the steps;

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

3) 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;

4) 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~~ URI to be contacted into the Route header as the topmost entry followed by its own ~~URL~~ URI populated as specified in the subclause 5.4.3.4; and

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

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

6) insert an orig-ioi parameter into the P-Charging-Vector header. The S-CSCF shall set the orig-ioi parameter to a value that identifies the sending network. The S-CSCF shall not include the term-ioi parameter;

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

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

9) 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~~ URI 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 to the originator;

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

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

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

13) in case the request is forwarded to the destination network (either via an I-CSCF(THIG) or directly), remove the P-Access-Network-Info header; ~~and~~

14) route the request based on SIP routeing procedures; and~~.~~

15) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;

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, if the response corresponds to an INVITE request, ~~it~~ the S-CSCF shall save the ~~necessary~~ Contact and Record-Route header field~~s~~ values ~~and the Contact header from~~ in the response in order to be able to release the ~~dialog~~ session if needed.

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

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

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

3) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;

~~3~~4) in case the request is forwarded to the destination network or to an AS located outside the trust domain, remove the P-Access-Network-Info header; and

~~4~~5) route the request based on the topmost Route header.

When the S-CSCF receives a response to the target refresh request for a dialog, if the response corresponds to an INVITE request, ~~it~~ the S-CSCF shall save the Contact and~~necessary~~ Record-Route header ~~fields~~ field values ~~and the Contact header from~~ in the response ~~in order to~~such that the S-CSCF is able to release the ~~dialog~~ session if needed.

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

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

2) in case the request is forwarded to the destination network or to an AS located outside the trust domain, remove the P-access-network-info header; and

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

Next proposed change

5.4.3.3 Requests terminated at the served user

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

1) determine whether the request contains a barred public user identity in the Request-URI of the request or not. In case the Request URI contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 404 (Not Found) response. Otherwise, continue with the rest of the steps;

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

3) 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;

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

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

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

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;

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

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

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

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

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

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

13) if the request is an INVITE request, save the Contact, CSeq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed; and ~~in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary Record-Route header fields and the Contact header from the request in order to release the dialog when needed; and~~

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

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

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

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

1) execute the procedures described in the steps 1, 2 and 3 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction);

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

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

4) execute the procedure described in step 4 and 5 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

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

5) execute the procedures described in the steps 6, 7, 12, 13, 14 and 15 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

When the S-CSCF receives a response to the initial request for a dialog (whether the user is registered or not), it shall:

1) ~~-~~if the response corresponds to an INVITE request, save the ~~necessary ~~Contact and Record-Route header field~~s~~ values ~~and the Contact header field from~~in the response ~~in order to~~such that the S-CSCF is able to release the ~~dialog ~~seession if needed;~~.~~

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

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

When the S-CSCF receives a response to a request for a standalone transaction (whether the user is registered or not), in the case where the S-CSCF has knowledge of an associated tel-~~URI ~~URL for a SIP ~~URL ~~URI contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel-~~URI~~URL. In case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header.

When the S-CSCF receives the 200 (OK) response for a standalone transaction request, the S-CSCF shall insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards an AS.

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

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

2) if the request is an INVITE request, save the Contact, Cseq and Record-Route header field values received in the request such that the S-CSCF is able to release the session if needed;

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

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

When the S-CSCF receives a response to the target refresh request for a dialog (whether the user is registered or not), ~~it ~~the S-CSCF shall:

1) if the response corresponds to an INVITE request, save the ~~necessary ~~Record-Route and Contact header field~~s~~ values ~~and the Contact header field from~~in the response~~ in order to ~~ such that the S-CSCF is able to release the ~~dialog ~~session if needed;~~.~~

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

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

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

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

When the S-CSCF receives a response to a a subsequent request other than target refresh request for a dialog, in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header.

3GPP TSG-CN1 Meeting #30 **Tdoc N1-030858**
San Diego, California, USA, 19 – 23 May 2003 **was N1-030592**

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **371** ⌘**rev** **1** ⌘ Current version: **5.4.0** ⌘

*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:	⌘	Profile Tables - Transparency
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	21.05.03
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:	⌘	Some readers of Annex A in 24.229 interpreted the Profile Tables as if they would state that CSCFs and AS's when acting as a SIP Proxy, would not be transparen in the same way as defined for SIP Proxies. It can be understood from the text and the tables in Annex A, that IMS is not transparent to unknown SIP elements (headers, parameters and messages).
Summary of change:	⌘	It is clearly stated in Annex A, that CSCFs and AS's when performing the SIP Proxy role are transparent as defined in RFC 3261
Consequences if not approved:	⌘	24.229 is misunderstood by reader. Wrong implementation. 24.229 is out-of-line with RFC 3261 / SIP Problems when creating services on top of IMS Further IETF Liaisons

Clauses affected:	⌘	Annex A

Other specs affected: ⌘

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

Other comments:	⌘	In case of conflicts with tdoc N1-030593 ("Profile Tables – Terminology"), the changes made in this CR shall take precedence, i.e. the changes made in N1-030593 shall be overruled by this CR in case of conflict.

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 and only Change

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

A.1 Profiles

A.1.1 Relationship to other specifications

This annex contains a profile to the IETF specifications which are referenced by this specification, and the PICS proformas underlying profiles do not add requirements to the specifications they are proformas for.

This annex provides a profile specification according to both the current IETF specifications for SIP, SDP and other protocols (as indicated by the "RFC status" column in the tables in this annex) which are referenced by this specification and to the 3GPP specifications using SIP (as indicated by the "Profile status" column in the tables in this annex.

In the "RFC status" column the contents of the referenced specification takes precedence over the contents of the entry in the column. However, a number of the referenced specifications reference RFC 2543 rather than RFC 3261 [26], and therefore certain extensions (particularly new headers) have not been included in these referenced specifications. 3GPP apply the extensions of the bis draft to IETF specifications that reference RFC 2543, and where this consideration applies to the entry in the "RFC status" column, then the entry should apply and override the referenced IETF specification.

In the "Profile status" column, there are a number of differences from the "RFC status" column. Where these differences occur, these differences take precedence over any requirements of the IETF specifications. Where specification concerning these requirements exists in the main body of the present document, the main body of the present document takes precedence.

Where differences occur in the "Profile status" column, the "Profile status" normally gives more strength to a "RFC status" and is not be in contradiction with the "RFC status", e.g. it may change an optional "RFC status" to a mandatory "Profile status". If the "Profile status" weakens the strength of a "RFC status" then additionally this will be indicated by further textual description in the present document.

For all IETF specifications that are not referenced by this document or that are not mentioned within the 3GPP profile of SIP and SDP, the generic rules as defined by RFC 3261 [26] and in addition the rules in clauses 5 and 6 of this specification apply, e.g..

- a proxy which is built in accordance to this specification passes on any unknown method, unknown header field or unknown header parameter after applying procedures such as filtering, insertion of P-Asserted-Identity header, etc.;
- an UA which is built in accordance to this specification will
  - handle received unknown methods in accordance to the procedures defined in RFC 3261 [26], e.g. respond with a 400 (Bad Request) response; and
  - handle unknown header fields and unknown header parameters in accordance to the procedures defined in RFC 3261 [26], e.g. respond with a 420 (Bad Extension) if an extension identified by an option tag in the Require header of the received request is not supported by the UA.

A.1.2 Introduction to methodology within this profile

This subclause does not reflect dynamic conformance requirements but static ones. In particular, an condition for support of a PDU parameter does not reflect requirements about the syntax of the PDU (i.e. the presence of a parameter) but the capability of the implementation to support the parameter.

In the sending direction, the support of a parameter means that the implementation is able to send this parameter (but it does not mean that the implementation always sends it).

In the receiving direction, it means that the implementation supports the whole semantic of the parameter that is described in the main part of this specification.

As a consequence, PDU parameter tables in this subclause are not the same as the tables describing the syntax of a PDU in the reference specification, e.g. RFC 3261 [26] tables 2 and 3. It is not rare to see a parameter which is optional in the syntax but mandatory in subclause below.

The various statii used in this subclause are in accordance with the rules in table A.1.

Table A.1: Key to status codes

Status code	Status name	Meaning
M	mandatory	the capability shall be supported. It is a static view of the fact that the conformance requirements related to the capability in the reference specification are mandatory requirements. This does not mean that a given behaviour shall always be observed (this would be a dynamic view), but that it shall be observed when the implementation is placed in conditions where the conformance requirements from the reference specification compel it to do so. For instance, if the support for a parameter in a sent PDU is mandatory, it does not mean that it shall always be present, but that it shall be present according to the description of the behaviour in the reference specification (dynamic conformance requirement).
O	optional	the capability may or may not be supported. It is an implementation choice.
n/a	not applicable	it is impossible to use the capability. No answer in the support column is required.
x	prohibited (excluded)	it is not allowed to use the capability. This is more common for a profile.
c <integer>	conditional	the requirement on the capability ("m", "o", "n/a" or "x") depends on the support of other **optional or conditional** items. <integer> is the identifier of the conditional expression.
o.<integer>	qualified optional	for mutually exclusive or selectable options from a set. <integer> is the identifier of the group of options, and the logic of selection of the options.
i	irrelevant	capability outside the scope of the given specification. Normally, this notation should be used in a base specification ICS proforma only for transparent parameters in received PDUs. However, it may be useful in other cases, when the base specification is in fact based on another standard.

In the context of this specification the "i" status code mandates that the implementation does not change the content of the parameter. It is an implementation option if the implementation acts upon the content of the parameter (e.g. by setting filter criteria to known or unknown parts of parameters in order to find out the route a message has to take).

It must be understood, that this 3GPP SIP profile does not list all parameters which an implementation will treat as indicated by the status code "irrelevant". In general an implementation will pass on all unknown messages, header fields and header parameters, as long as it can perform its normal behaviour.

The following additional comments apply to the interpretation of the tables in this Annex.

NOTE 1: The tables are constructed according to the conventional rules for ICS proformas and profile tables.

NOTE 2: The notation (either directly or as part of a conditional) of "m" for the sending of a parameter and "i" for the receipt of the same parameter, may be taken as indicating that the parameter is passed on transparently, i.e. without modification. Where a conditional applies, this behaviour only applies when the conditional is met.

A.1.3 Roles

Table A.2: Roles

Item	Roles	Reference	RFC status	Profile status
1	User agent	[26]	o.1	o.1
2	Proxy	[26]	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	5.1	n/a	o.1
2	P-CSCF	5.2	n/a	o.1
3	I-CSCF	5.3	n/a	o.1
3A	I-CSCF (THIG)	5.3	n/a	c1
4	S-CSCF	5.4	n/a	o.1
5	BGCF	5.6	n/a	o.1
6	MGCF	5.5	n/a	o.1
7	AS	5.7	n/a	o.1
7A	AS acting as terminating UA, or redirect server	5.7.2	n/a	c2
7B	AS acting as originating UA	5.7.3	n/a	c2
7C	AS acting as a SIP proxy	5.7.4	n/a	c2
7D	AS performing 3rd party call control	5.7.5	n/a	c2
8	MRFC	5.8	n/a	o.1
c1: IF A.3/3 THEN o ELSE x - - I-CSCF. 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.				

3GPP TSG-CN1 Meeting #30
San Diego, California, USA, 19 – 23 May 2003

Tdoc N1-030860
was N1-030596

CR-Form-v7

CHANGE REQUEST

⌘	**24.229**	**CR**	**375**	⌘ **rev**	**1**	⌘	Current version:	**5.4.0** ⌘

*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:	⌘	Profile Tables – Major Capability Corrections
Source:	⌘	Nokia
Work item code:	⌘	IMS-CCR
Date:	⌘	28.04.03
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 following problems have been identified in the Major Capabilitiy Tables in Annex A of 24.229:

General

1) The detailed refererences in the Reference column were not checked

UE Major Capabilities:

2) item A.4/3 and /4: client /server behviour for INVITE requests – set to "o" (optional), although later on "100rel" (item 14) and "UPDATE" (item 17) are indicated as "m" (mandatory). 100rel and Update cannot be used if INVITE is not supported. Therefore a new item A.4/2A is added which refers to the capability of "initiating sessions" – which is optional. All other session related items show now a condition for this item.

5) item A.4/19: SIP extensions for media authorization – this is only required to be supported by the UE and the P-CSCF, e.g. S-CSCF when performing the SIP UA role does not need to support this -> therefore a condition was added (c.14)

6) item A.4/21: Use of NOTIFY to establish a dialog – not regarded as major capability (anyhow mandatory if RFC 3265 is supported) -> crossed out

7) item A.4/22 – Acting as the Notifier of Event Information – UE does not need to act as event notifier, only S-CSCF, therefore c.15 was added.

8) item A.4/22 – Acting as the subscriber to event information – this is a role that

currently only P-CSCF and UE need to perform, therefore c.16 was added

12) item A.4/27 – a messaging mechanism for SIP – the Message method is not mandated to be supported in the UE role in any IMS entity – the S-CSCF may only generate it. Therefore the condition (c.7) was changed.

13) item A.4/28 – SIP extension header field for service route discovery during registration – this is (in UE role) only supported by S-CSCF and UE, therefore c.17 was added.

Please note also the minor changes in the "PDU" tables (A.5) which are direct consequences of the changes as described above.

Proxy Major Capabilities:

14) item A.162/1 and A.162/2 – client/server behaviour for session requests – the terminology here is chosen in an unhappy way, as the reader tends to understand this as "being able to send/receive INVITE messages as a UE" – the statements were rephrased

15) item A.162/3 – session release – of course a SIP Proxy does not support sending of session release related messages, therefore the RFC status changed from mandatory to eXcluded, whilst it was added as mandatory for S-CSCF and P-CSCF (c.14).

16) item A.162/4 – stateless proxy behaviour – only I-CSCF may act as stateless proxy, c.15 was added

17) item A.162/5 – stateful proxy behaviour – all CSCFs may act as stateful proxies, P-/S-CSCF must act as stateful proxies, c.16 was added

19) item A.162/14 – record-routing - is mandatory S-/P-/I-CSCF, c2 deleted

21) Item A.162/21 – reliability of provisional responses – there is no action performed in a proxy for any 100rel related message or header, it is true that the CSCFs need to transport it transparently, but that's all – the "m" is changed to an "i"

22) Item A.162/23 – resource management – same reasoning as under 21)

23) Item A.162/24 – UPDATE method – same reasoingn as under 21)

24) Item A.162/26 – SIP extensions for media authorization – this only needs to be supported by the P-CSCF, c.7 re-used

25) Item A.162/27 – SIP specific Event Notification – why this is set to optional? In the thinking of the tables as they were edited up till now – as it was understood by the editor of this CR – this should be "m"andatory, as a CSCF needs to implement transparency for it. Anyhow – CSCF needs to be transparent, therefore set to "i"

27) item A.162/30 – extension to SIP for asserted identity within trusted networks – it is understood that this extension only needs to be supported by S-/P-CSCF, c.17 added

29) item A.162/32 – Service-Route – no, this is not mandated to be supported by P- and I-CSCF, that’s simply wrong. Even an "o" is wrong here, it's just "i". RTFM

Summary of change:	⌘	The above listed problems are corrected	
Consequences if not approved:	⌘	Major Capability Tables are not in-line with the protocol text in 3GPP TS's and SIP RFCs – means that they are not useful.	

Clauses affected:	⌘	Annex A				
		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 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
2A	initiating a session?	[26] subclause 13	o	o
3	client behaviour for INVITE requests?	[26] subclause 13.2	c18	c18
4	server behaviour for INVITE requests?	[26] subclause 13.3	c18	c18
5	session release?	[26] subclause 15.1	c18	c18
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
8A	authentication between UA and proxy?	[26] 20.28, 22.3	o	o
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]	c19	c18
15	the REFER method?	[36]	o	o
16	integration of resource management and SIP?	[30]	c19	c18
17	the SIP UPDATE method?	[29]	c5	c18
19	SIP extensions for media authorization?	[31]	o	c14
20	SIP specific event notification?	[28]	o	c13
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	c15
23	acting as the subscriber to event information?	[28]	c2	c16
24	session initiation protocol extension header field for registering non-adjacent contacts?	[35]	o	c6
25	private 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
26A	request of privacy by the inclusion of a Privacy header	[33]	c9	c11
26B	application of privacy based on the received Privacy header	[33]	c9	n/a
26C	passing on of the Privacy header transparently	[33]	c9	c12
26D	application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the assistance of intermediaries are obscured?	[33] 5.1	c10	
26E	application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs?	[33] 5.2	c10	
26F	application of the privacy option "user"	[33] 5.3	c10	

	such that user level privacy functions are provided by the network?			
26G	application of the privacy option "id" such that privacy of the network asserted identity is provided by the network?	[34] 7	c10	n/a
27	a messaging mechanism for the Session Initiation Protocol (SIP)?	[50]	o	c7
28	session initiation protocol extension header field for service route discovery during registration?	[38]	o	c17
29	compressing the session initiation protocol?	[55]	o	c8

c2: IF A.4/20 THEN o.1 ELSE n/a - - SIP specific event notification extension.
c3: IF A.3/1 OR A.3/4 THEN m ELSE n/a - - UE 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 extension.
c6: IF A.3/4 OR A.3/1 THEN m ELSE n/a. - - S-CSCF or UE.
c7: IF A.3/4 THEN m ELSE (IF A.3/1 OR A.3/7B OR A.3/7D THEN o ELSE n/a) - - S-CSCF or UA or AS acting as originating UA, or AS performing 3rd party call controlc8: IF A.3/1 THEN m ELSE n/a - - UE behaviour.
c9: IF A.4/26 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c10: IF A.4/26B THEN o.3 ELSE n/a - - application of privacy based on the received Privacy header.
c11: IF A.3/1 OR A.3/6 THEN o ELSE n/a - - UE or MGCF.
c12: IF A.3/7D THEN m ELSE n/a - - AS performing 3rd-party call control.
c13: IF A.3/1 OR A.3/4 THEN m ELSE o - - UE behaviour or S-CSCF.
c14: IF A.3/1 THEN m ELSE IF A.3/2 THEN o ELSE n/a – UE or P-CSCF
c15: IF A.4/20 and A.3/4 THEN m ELSE o – SIP specific event notification extensions and S-CSCF.
c16: IF A.4/20 and (A.3/1 OR A.3/2) THEN m ELSE o - - SIP specific event notification extension and UE or P-CSCF.
c17: IF A.3/1 o A3./4 THEN m ELSE n/a – UE or S-CSCF
c18: IF A.4/2A THEN m ELSE n/a - - initiating sessions
c19: IF A.4/2A THEN o ELSE n/a - - initiating sessions
o.1: At least one of these capabilities is supported.
o.2: At least one of these capabilities is supported.
o.3: At least one of these capabilities is supported.

Second and last 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			
3	initiate session release?	[26] 16	x	c14
4	stateless proxy behaviour?	[26] 16.11	o.1	c15
5	stateful proxy behaviour?	[26] 16.2	o.1	c16
6	forking of initial requests?	[26] 16.1	c1	x
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
8A	authentication between UA and proxy?	[26] 20.28, 22.3	o	x
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	being able to insert itself in the subsequent transactions in a dialog (record-routing)?	[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
19A	reading the contents of the Organization header before proxying the request or response?	[26] 20.25	o	o
19B	adding or concatenating the Organization header before proxying the request or response?	[26] 20.25	o	o
19C	reading the contents of the Call-Info header before proxying the request or response?	[26] 20.25	o	o
19D	adding or concatenating the Call-Info header before proxying the request or response?	[26] 20.25	o	o
19E	delete Contact headers from 3xx responses prior to relaying the response?	[26] 20	o	o
	Extensions			

20	the SIP INFO method?	[25]	o	o
21	reliability of provisional responses in SIP?	[27]	o	i
22	the REFER method?	[36]	o	o
23	integration of resource management and SIP?	[30]	o	i
24	the SIP UPDATE method?	[29]	c4	i
26	SIP extensions for media authorization?	[31]	o	c7
27	SIP specific event notification	[28]	o	i
28	the use of NOTIFY to establish a dialog	[28] 4.2	o	n/a
29	Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts	[35]	o	c6
30	extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks	[34]	o	m
30A	act as first entity within the trust domain for asserted identity	[34]	c5	c8
30B	act as subsequent entity within trust network that can route outside the trust network	[34]	c5	c9
31	a privacy mechanism for the Session Initiation Protocol (SIP)	[33]	o	m
31A	request of privacy by the inclusion of a Privacy header	[33]	n/a	
31B	application of privacy based on the received Privacy header	[33]	c10	
31C	passing on of the Privacy header transparently	[33]	c10	
31D	application of the privacy option "header" such that those headers which cannot be completely expunged of identifying information without the assistance of intermediaries are obscured?	[33] 5.1	x	
31E	application of the privacy option "session" such that anonymization for the session(s) initiated by this message occurs?	[33] 5.2	n/a	n/a
31F	application of the privacy option "user" such that user level privacy functions are provided by the network?	[33] 5.3	n/a	n/a
31G	application of the privacy option "id" such that privacy of the network asserted identity is provided by the network?	[34] 7	c11	c12
32	Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration	[38]	o	i17
33	a messaging mechanism for the Session Initiation Protocol (SIP)	[50]	o	m
34	Compressing the Session Initiation Protocol	[55]	o	c7

c1:	IF A.162/5 THEN o ELSE n/a - - stateful proxy behaviour.
c2:	IF A.3/2 OR A.3/3A OR A.3/4 THEN m ELSE o- - P-CSCF, I-CSCF(THIG) or S-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.162/30 THEN o ELSE n/a - - extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c6:	IF A.3/2 OR A.3/3A THEN m ELSE n/a - - P-CSCF or I-CSCF (THIG).
c7:	IF A.3/2 THEN m ELSE n/a - - P-CSCF.
c8:	IF A.3/2 AND A.162/30 THEN m ELSE n/a - - P-CSCF and extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.
c9:	
c10:	IF A.162/31 THEN o.2 ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c11:	IF A.162/31B THEN o ELSE x - - application of privacy based on the received Privacy header.
c12:	
c13:	
c14	IF A.3/2 OR A.3/4 THEN m ELSE x - - P-CSCF or S-CSCF
c15	IF A.3/2 OR A.3/4 OR A.3/6 then m ELSE o - - P-CSCF or S-CSCF of MGCF
c16	IF A.3/2 OR A.3/4 OR A.3/6 then o ELSE m - - P-CSCF or S-CSCF of MGCF
c17	IF A.3/2 o ELSE i - - P-CSCF
o.1:	It is mandatory to support at least one of these items.
o.2:	It is mandatory to support at least one of these items.
NOTE:	An AS acting as a proxy may be outside the trust domain, and therefore not able to support the capability for that reason; in this case it is perfectly reasonable for the header to be passed on transparently, as specified in the PDU parts of the profile.

3GPP TSG-CN1 Meeting #30 **Tdoc N1-030921**
San Diego, California, USA, 19 – 23 May 2003 **was N1-030597, N1-030894**

CR-Form-v7

CHANGE REQUEST

⌘	**24.229**	**CR**	**376**	⌘ **rev**	**2**	⌘	Current version:	**5.4.0** ⌘

*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:	⌘	Profile Tables – Deletion of Elements not used in 24.229		
Source:	⌘	Nokia		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	28.04.03
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:	⌘	24.229 Profile Tables shall only list SIP / SDP messages, headers and parameters, that are used within 24.229
Summary of change:	⌘	Deletion of all SIP / SDP messages, headers and parameters that are not used within 24.229 in the Profile Tables of Annex A.
Consequences if not approved:	⌘	Reader will assume that CSCFs are not transparent for SIP signaling that is not listed in the 24.229 Profile Tables. Therefore 24.229 would be not in-line with SIP, as SIP proxies are transparent for all SIP signaling that is unknown to them. -> Wrong implementations.

Clauses affected:	⌘	2, Annex A				
		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 Change

A.1.1 Relationship to other specifications

This annex contains a profile to the IETF specifications, and the PICS proformas underlying profiles do not add requirements to the specifications they are proformas for.

This annex provides a profile specification according to both the current IETF specifications for SIP, SDP and other protocols (as indicated by the "RFC status" column in the tables in this annex) and to the 3GPP specifications using SIP (as indicated by the "Profile status" column in the tables in this annex.

In the "RFC status" column the contents of the referenced specification takes precedence over the contents of the entry in the column. ~~However, a number of the referenced specifications reference RFC 2543 rather than RFC 3261 [26], and therefore certain extensions (particularly new headers) have not been included in these referenced specifications. 3GPP apply the extensions of the bis draft to IETF specifications that reference RFC 2543, and where this consideration applies to the entry in the "RFC status" column, then the entry should apply and override the referenced IETF specification.~~

In the "Profile status" column, there are a number of differences from the "RFC status" column. Where these differences occur, these differences take precedence over any requirements of the IETF specifications. Where specification concerning these requirements exists in the main body of the present document, the main body of the present document takes precedence.

Where differences occur in the "Profile status" column, the "Profile status" normally gives more strength to a "RFC status" and is not be in contradiction with the "RFC status", e.g. it may change an optional "RFC status" to a mandatory "Profile status". If the "Profile status" weakens the strength of a "RFC status" then additionally this will be indicated by further textual description in the present document.

NOTE 1: The referenced specifications consist of the set of IETF specifications that existed at the time of freezing of this document. Further extensions continue to be specified to SIP, SDP and other protocols, and profiles detailing the support or absence of support of these will not be specified in this major version. An exception exists where the extension specifies functionality that had been agreed by stage 1 and stage 2 to be included in this major version (where the related IETF draft had not been completed in time).

NOTE 2: Absence of a referenced specification does not necessarily preclude the use end-to-end by the UE or AS of such an extension. However, the UE or AS cannot depend on the support of such an extension by other functional entities within the IM CN subsystem within this major version.

Second Change

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 - - the REFER method extension.
~~c2: IF A.4/13 THEN m ELSE n/a - - the SIP INFO method extension.~~
c3: IF A.4/23 THEN m ELSE n/a - - recipient for event information.
c4: IF A.4/22 THEN m ELSE n/a - - notifier of event information.
c5: IF A.4/14 THEN m ELSE n/a - - reliability of provisional responses extension.
c6: IF A.4/17 THEN m ELSE n/a - - the SIP update method extension.
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 Change

A.2.1.4.6 ~~INFO method~~Void

~~Prerequisite A.5/6 - - INFO request~~

~~**Table A.32: Supported headers within the INFO request**~~

~~**Item**~~	~~**Header**~~	~~**Sending**~~			~~**Receiving**~~		
		~~**Ref.**~~	~~**RFC status**~~	~~**Profile status**~~	~~**Ref.**~~	~~**RFC status**~~	~~**Profile status**~~
~~1~~	~~Accept~~	~~[26] 20.1~~	~~o~~	~~o~~	~~[26] 20.1~~	~~m~~	~~m~~
~~2~~	~~Accept-Encoding~~	~~[26] 20.2~~	~~o~~	~~o~~	~~[26] 20.2~~	~~m~~	~~m~~
~~3~~	~~Accept-Language~~	~~[26] 20.3~~	~~o~~	~~o~~	~~[26] 20.3~~	~~m~~	~~m~~
~~3A~~	~~Allow~~	~~[26] 20.5~~	~~o~~	~~o~~	~~[26] 20.5~~	~~m~~	~~m~~
~~4~~	~~Allow-Events~~	~~[28] 8.2.2~~	~~c1~~	~~c1~~	~~[28] 8.2.2~~	~~c2~~	~~c2~~
~~5~~	~~Authorization~~	~~[26] 20.7~~	~~c3~~	~~c3~~	~~[26] 20.7~~	~~c3~~	~~c3~~
~~6~~	~~Call-ID~~	~~[26] 20.8~~	~~m~~	~~m~~	~~[26] 20.8~~	~~m~~	~~m~~
~~7~~	~~Contact~~	~~[26] 20.10~~	~~o~~	~~o~~	~~[26] 20.10~~	~~o~~	~~o~~
~~7A~~	~~Content-Disposition~~	~~[26] 20.11~~	~~o~~	~~o~~	~~[26] 20.11~~	~~m~~	~~m~~
~~8~~	~~Content-Encoding~~	~~[26] 20.12~~	~~o~~	~~o~~	~~[26] 20.12~~	~~m~~	~~m~~
~~8A~~	~~Content-Language~~	~~[26] 20.13~~	~~o~~	~~o~~	~~[26] 20.13~~	~~m~~	~~m~~
~~9~~	~~Content-Length~~	~~[26] 20.14~~	~~m~~	~~m~~	~~[26] 20.14~~	~~m~~	~~m~~
~~10~~	~~Content-Type~~	~~[26] 20.15~~	~~m~~	~~m~~	~~[26] 20.15~~	~~m~~	~~m~~
~~11~~	~~Cseq~~	~~[26] 20.16~~	~~m~~	~~m~~	~~[26] 20.16~~	~~m~~	~~m~~
~~12~~	~~Date~~	~~[26] 20.17~~	~~c4~~	~~c4~~	~~[26] 20.17~~	~~m~~	~~m~~
~~14~~	~~From~~	~~[26] 20.20~~	~~m~~	~~m~~	~~[26] 20.20~~	~~m~~	~~m~~
~~15~~	~~Max-Forwards~~	~~[26] 20.22~~	~~o~~	~~o~~	~~[26] 20.22~~	~~n/a~~	~~n/a~~
~~15A~~	~~MIME-Version~~	~~[26] 20.24~~	~~o~~	~~o~~	~~[26] 20.24~~	~~m~~	~~m~~
~~16~~	~~Organization~~	~~[26] 20.25~~	~~o~~	~~o~~	~~[26] 20.25~~	~~o~~	~~o~~
~~17~~	~~Priority~~	~~[26] 20.26~~	~~o~~	~~o~~	~~[26] 20.26~~	~~o~~	~~o~~
~~17A~~	~~Privacy~~	~~[33] 4.2~~	~~c6~~	~~n/a~~	~~[33] 4.2~~	~~c6~~	~~n/a~~
~~18~~	~~Proxy-Authorization~~	~~[26] 20.28~~	~~c5~~	~~c5~~	~~[26] 20.28~~	~~n/a~~	~~n/a~~
~~19~~	~~Proxy-Require~~	~~[26] 20.29~~	~~o~~	~~n/a~~	~~[26] 20.29~~	~~n/a~~	~~n/a~~
~~20~~	~~Record-Route~~	~~[26] 20.30~~	~~n/a~~	~~n/a~~	~~[26] 20.30~~	~~n/a~~	~~n/a~~
~~21~~	~~Require~~	~~[26] 20.32~~	~~o~~	~~o~~	~~[26] 20.32~~	~~m~~	~~m~~
~~22~~	~~Route~~	~~[26] 20.34~~	~~m~~	~~m~~	~~[26] 20.34~~	~~n/a~~	~~n/a~~
~~23~~	~~Subject~~	~~[26] 20.36~~	~~o~~	~~o~~	~~[26] 20.36~~	~~o~~	~~o~~
~~24~~	~~Supported~~	~~[26] 20.37~~	~~o~~	~~o~~	~~[26] 20.37~~	~~m~~	~~m~~
~~25~~	~~Timestamp~~	~~[26] 20.38~~	~~c8~~	~~c8~~	~~[26] 20.38~~	~~m~~	~~m~~
~~26~~	~~To~~	~~[26] 20.39~~	~~m~~	~~m~~	~~[26] 20.39~~	~~m~~	~~m~~
~~27~~	~~User-Agent~~	~~[26] 20.41~~	~~o~~	~~o~~	~~[26] 20.41~~	~~o~~	~~o~~
~~28~~	~~Via~~	~~[26] 20.42~~	~~m~~	~~m~~	~~[26] 20.42~~	~~m~~	~~m~~

~~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.4/8A THEN m ELSE n/a - - authentication between UA and proxy.~~

~~c6: IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).~~

~~c8: IF A.4/6 THEN o ELSE n/a - - timestamping of requests.~~

~~Prerequisite A.5/6 - - INFO request~~

~~**Table A.33: Supported message bodies within the INFO request**~~

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

~~Prerequisite A.5/7 - - INFO response~~

~~Prerequisite: A.6/1 - - 100 (Trying)~~

~~Table A.34: Supported headers within the INFO response~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~1~~	~~Call-ID~~	~~[26] 20.8~~	~~n/a~~	~~n/a~~	~~[26] 20.8~~	~~m~~	~~m~~
~~2~~	~~Content-Length~~	~~[26] 20.14~~	~~n/a~~	~~n/a~~	~~[26] 20.14~~	~~m~~	~~m~~
~~3~~	~~Cseq~~	~~[26] 20.16~~	~~n/a~~	~~n/a~~	~~[26] 20.16~~	~~m~~	~~m~~
~~4~~	~~Date~~	~~[26] 20.17~~	~~n/a~~	~~n/a~~	~~[26] 20.17~~	~~m~~	~~m~~
~~5~~	~~From~~	~~[26] 20.20~~	~~n/a~~	~~n/a~~	~~[26] 20.20~~	~~m~~	~~m~~
~~6~~	~~To~~	~~[26] 20.39~~	~~n/a~~	~~n/a~~	~~[26] 20.39~~	~~m~~	~~m~~
~~7~~	~~Via~~	~~[26] 20.42~~	~~n/a~~	~~n/a~~	~~[26] 20.42~~	~~m~~	~~m~~

~~Prerequisite A.5/7 - - INFO response~~

~~Table A.35: Supported headers within the INFO 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~~
~~1A~~	~~Content-Disposition~~	~~[26] 20.11~~	~~o~~	~~o~~	~~[26] 20.11~~	~~m~~	~~m~~
~~2~~	~~Content-Encoding~~	~~[26] 20.12~~	~~o~~	~~o~~	~~[26] 20.12~~	~~m~~	~~m~~
~~2A~~	~~Content-Language~~	~~[26] 20.13~~	~~o~~	~~o~~	~~[26] 20.13~~	~~m~~	~~m~~
~~3~~	~~Content-Length~~	~~[26] 20.14~~	~~m~~	~~m~~	~~[26] 20.14~~	~~m~~	~~m~~
~~4~~	~~Content-Type~~	~~[26] 20.15~~	~~m~~	~~m~~	~~[26] 20.15~~	~~m~~	~~m~~
~~5~~	~~Cseq~~	~~[26] 20.16~~	~~m~~	~~m~~	~~[26] 20.16~~	~~m~~	~~m~~
~~6~~	~~Date~~	~~[26] 20.17~~	~~c1~~	~~c1~~	~~[26] 20.17~~	~~m~~	~~m~~
~~7~~	~~From~~	~~[26] 20.20~~	~~m~~	~~m~~	~~[26] 20.20~~	~~m~~	~~m~~
~~7A~~	~~MIME-Version~~	~~[26] 20.24~~	~~o~~	~~o~~	~~[26] 20.24~~	~~m~~	~~m~~
~~8~~	~~Organization~~	~~[26] 20.25~~	~~o~~	~~o~~	~~[26] 20.25~~	~~m~~	~~m~~
~~8A~~	~~Privacy~~	~~[33] 4.2~~	~~c3~~	~~n/a~~	~~[33] 4.2~~	~~c3~~	~~n/a~~
~~8B~~	~~Server~~	~~[26] 20.35~~	~~o~~	~~o~~	~~[26] 20.35~~	~~o~~	~~o~~
~~9~~	~~Timestamp~~	~~[26] 20.38~~	~~m~~	~~m~~	~~[26] 20.38~~	~~c2~~	~~c2~~
~~10~~	~~To~~	~~[26] 20.39~~	~~m~~	~~m~~	~~[26] 20.39~~	~~m~~	~~m~~
~~10A~~	~~User-Agent~~	~~[26] 20.41~~	~~o~~	~~o~~	~~[26] 20.41~~	~~o~~	~~o~~
~~11~~	~~Via~~	~~[26] 20.42~~	~~m~~	~~m~~	~~[26] 20.42~~	~~m~~	~~m~~
~~12~~	~~Warning~~	~~[26] 20.43~~	~~o (note)~~	~~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.~~						
~~c3:~~	~~IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).~~						
~~NOTE:~~	~~For a 606 (Not Acceptable Here) response, this status is RECOMMENDED rather than OPTIONAL.~~						

~~Prerequisite A.5/7 - - INFO response~~

~~Prerequisite: A.6/6 - - 2xx~~

~~Table A.36: Supported headers within the INFO response~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~1~~	~~Allow~~	~~[26] 20.5~~	~~o~~	~~o~~	~~[26] 20.5~~	~~m~~	~~m~~
~~2~~	~~Authentication-Info~~	~~[26] 20.6~~	~~c1~~	~~c1~~	~~[26] 20.6~~	~~c2~~	~~c2~~
~~5~~	~~Require~~	~~[26] 20.32~~	~~m~~	~~m~~	~~[26] 20.32~~	~~m~~	~~m~~
~~7~~	~~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.5/7 - - INFO response~~

~~Prerequisite: A.6/8 OR A.6/9 OR A.6/10 OR A.6/11 OR A.6/12 - - 3xx~~

~~Table A.37: Supported headers within the INFO response~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Allow~~	~~[26] 20.5~~	~~o~~	~~o~~	~~[26] 20.5~~	~~m~~	~~m~~
~~1~~	~~Error-Info~~	~~[26] 20.18~~	~~o~~	~~o~~	~~[26] 20.18~~	~~o~~	~~o~~
~~3~~	~~Require~~	~~[26] 20.32~~	~~m~~	~~m~~	~~[26] 20.32~~	~~m~~	~~m~~
~~5~~	~~Supported~~	~~[26] 20.37~~	~~m~~	~~m~~	~~[26] 20.37~~	~~m~~	~~m~~

~~Prerequisite A.5/7 - - INFO response~~

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

~~Table A.38: Supported headers within the INFO response~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Allow~~	~~[26] 20.5~~	~~o~~	~~o~~	~~[26] 20.5~~	~~m~~	~~m~~
~~1~~	~~Error-Info~~	~~[26] 20.18~~	~~o~~	~~o~~	~~[26] 20.18~~	~~o~~	~~o~~
~~2~~	~~Proxy-Authenticate~~	~~[26] 20.27~~	~~c1~~	~~c1~~	~~[26] 20.27~~	~~c1~~	~~c1~~
~~3~~	~~Require~~	~~[26] 20.32~~	~~m~~	~~m~~	~~[26] 20.32~~	~~m~~	~~m~~
~~5~~	~~Supported~~	~~[26] 20.37~~	~~m~~	~~m~~	~~[26] 20.37~~	~~m~~	~~m~~
~~8~~	~~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.5/7 - - INFO 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.39: Supported headers within the INFO response~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Allow~~	~~[26] 20.5~~	~~o~~	~~o~~	~~[26] 20.5~~	~~m~~	~~m~~
~~1~~	~~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~~
~~6~~	~~Supported~~	~~[26] 20.37~~	~~m~~	~~m~~	~~[26] 20.37~~	~~m~~	~~m~~

~~Prerequisite A.5/7 - - INFO response~~

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

~~Table A.40: Supported headers within the INFO 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~~
~~4~~	~~Require~~	~~[26] 20.32~~	~~m~~	~~m~~	~~[26] 20.32~~	~~m~~	~~m~~
~~6~~	~~Supported~~	~~[26] 20.37~~	~~m~~	~~m~~	~~[26] 20.37~~	~~m~~	~~m~~

~~Prerequisite A.5/7 - - INFO response~~

~~Prerequisite: A.6/14 - - 407 (Proxy Authentication Required)~~

~~Table A.40A: Supported headers within the INFO response~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~1~~	~~Allow~~	~~[26] 20.5~~	~~o~~	~~o~~	~~[26] 20.5~~	~~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.5/7 - - INFO response~~

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

~~Table A.41: Supported headers within the INFO response~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Accept~~	~~[26] 20.1~~	~~o.1~~	~~o.1~~	~~[26] 20.1~~	~~m~~	~~m~~
~~0B~~	~~Accept-Encoding~~	~~[26] 20.2~~	~~o.1~~	~~o.1~~	~~[26] 20.2~~	~~m~~	~~m~~
~~0C~~	~~Accept-Language~~	~~[26] 20.3~~	~~o.1~~	~~o.1~~	~~[26] 20.3~~	~~m~~	~~m~~
~~0D~~	~~Allow~~	~~[26] 20.5~~	~~o~~	~~o~~	~~[26] 20.5~~	~~m~~	~~m~~
~~1~~	~~Error-Info~~	~~[26] 20.18~~	~~o~~	~~o~~	~~[26] 20.18~~	~~o~~	~~o~~
~~3~~	~~Require~~	~~[26] 20.32~~	~~m~~	~~m~~	~~[26] 20.32~~	~~m~~	~~m~~
~~5~~	~~Supported~~	~~[26] 20.37~~	~~m~~	~~m~~	~~[26] 20.37~~	~~m~~	~~m~~
~~o.1~~	~~At least one of these capabilities is supported.~~						

~~Prerequisite A.5/7 - - INFO response~~

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

~~Table A.42: Supported headers within the INFO response~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Allow~~	~~[26] 20.5~~	~~o~~	~~o~~	~~[26] 20.5~~	~~m~~	~~m~~
~~1~~	~~Error-Info~~	~~[26] 20.18~~	~~o~~	~~o~~	~~[26] 20.18~~	~~o~~	~~o~~
~~3~~	~~Require~~	~~[26] 20.32~~	~~m~~	~~m~~	~~[26] 20.32~~	~~m~~	~~m~~
~~5~~	~~Supported~~	~~[26] 20.37~~	~~m~~	~~m~~	~~[26] 20.37~~	~~m~~	~~m~~
~~6~~	~~Unsupported~~	~~[26] 20.40~~	~~m~~	~~m~~	~~[26] 20.40~~	~~m~~	~~m~~

~~Prerequisite A.5/7 - - INFO response~~

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

~~**Table A.43: Supported headers within the INFO response**~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Allow~~	~~[26] 20.5~~	~~o~~	~~o~~	~~[26] 20.5~~	~~m~~	~~m~~
~~1~~	~~Error-Info~~	~~[26] 20.18~~	~~o~~	~~o~~	~~[26] 20.18~~	~~o~~	~~o~~
~~3~~	~~Require~~	~~[26] 20.32~~	~~m~~	~~m~~	~~[26] 20.32~~	~~m~~	~~m~~
~~5~~	~~Supported~~	~~[26] 20.37~~	~~m~~	~~m~~	~~[26] 20.37~~	~~m~~	~~m~~

~~Prerequisite A.5/7 - - INFO response~~

~~Prerequisite: A.6/35 - - 485 (Ambiguous")~~

~~**Table A.44: Supported headers within the INFO response**~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Allow~~	~~[26] 20.5~~	~~o~~	~~o~~	~~[26] 20.5~~	~~m~~	~~m~~
~~1~~	~~Error-Info~~	~~[26] 20.18~~	~~o~~	~~o~~	~~[26] 20.18~~	~~o~~	~~o~~
~~3~~	~~Require~~	~~[26] 20.32~~	~~m~~	~~m~~	~~[26] 20.32~~	~~m~~	~~m~~
~~5~~	~~Supported~~	~~[26] 20.37~~	~~m~~	~~m~~	~~[26] 20.37~~	~~m~~	~~m~~

~~Prerequisite A.5/7 - - INFO response~~

~~**Table A.45: Supported message bodies within the INFO response**~~

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

Fourth 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	c6	c6	[27] 6	c6	c6
15	PRACK response	[27] 6	c6	c6	[27] 6	c6	c6
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 - - the REFER method.
~~c2: IF A.162/20 THEN m ELSE n/a - - the SIP INFO method.~~
c3 IF A.162/27 THEN m ELSE n/a - - SIP specific event notification.
c4 IF A.162/24 THEN m ELSE n/a - - the SIP UPDATE method.
c5: IF A.162/33 THEN m ELSE n/a - - the SIP MESSAGE method.
c6: ÌF A.162/21 THEN m ELSE n/a - - reliability of provisional responses.

---

Fourth Change

---

A.2.2.4.6 ~~INFO method~~Void

~~Prerequisite A.163/6 - - INFO request~~

~~Table A.190: Supported headers within the INFO request~~

~~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~~
~~3A~~	~~Allow~~	~~[26] 20.5~~	~~m~~	~~m~~	~~[26] 20.5~~	~~i~~	~~i~~
~~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~~		~~[26] 20.8~~	~~m~~	
~~7~~	~~Contact~~	~~[26] 20.10~~	~~m~~	~~m~~	~~[26] 20.10~~	~~i~~	~~i~~
~~7A~~	~~Content-Disposition~~	~~[26] 20.11~~	~~m~~	~~m~~	~~[26] 20.11~~	~~i~~	~~c4~~
~~8~~	~~Content-Encoding~~	~~[26] 20.12~~	~~m~~	~~m~~	~~[26] 20.12~~	~~i~~	~~c4~~
~~8A~~	~~Content-Language~~	~~[26] 20.13~~	~~m~~	~~m~~	~~[26] 20.13~~	~~i~~	~~c4~~
~~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~~	~~c4~~
~~11~~	~~Cseq~~	~~[26] 20.16~~	~~m~~	~~m~~	~~[26] 20.16~~	~~m~~	~~m~~
~~12~~	~~Date~~	~~[26] 20.17~~	~~m~~	~~m~~	~~[26] 20.17~~	~~c2~~	~~c2~~
~~14~~	~~From~~	~~[26] 20.20~~	~~m~~	~~m~~	~~[26] 20.20~~	~~m~~	~~m~~
~~15~~	~~Max-Forwards~~	~~[26] 20.22~~	~~m~~	~~m~~	~~[26] 20.22~~	~~m~~	~~m~~
~~15A~~	~~MIME-Version~~	~~[26] 20.24~~	~~m~~	~~m~~	~~[26] 20.24~~	~~i~~	~~i~~
~~16~~	~~Organization~~	~~[26] 20.25~~	~~m~~	~~m~~	~~[26] 20.25~~	~~c3~~	~~c3~~
~~17~~	~~Priority~~	~~[26] 20.26~~	~~m~~	~~m~~	~~[26] 20.26~~	~~i~~	~~i~~
~~17A~~	~~Privacy~~	~~[33] 4.2~~	~~c9~~	~~c9~~	~~[33] 4.2~~	~~c10~~	~~c10~~
~~18~~	~~Proxy-Authorization~~	~~[26] 20.28~~	~~m~~	~~m~~	~~[26] 20.28~~	~~c8~~	~~c8~~
~~19~~	~~Proxy-Require~~	~~[26] 20.29~~	~~m~~	~~m~~	~~[26] 20.29~~	~~m~~	~~m~~
~~20~~	~~Record-Route~~	~~[26] 20.30~~	~~m~~	~~m~~	~~[26] 20.30~~	~~c7~~	~~c7~~
~~21~~	~~Require~~	~~[26] 20.32~~	~~m~~	~~m~~	~~[26] 20.32~~	~~c4~~	~~c5~~
~~22~~	~~Route~~	~~[26] 20.34~~	~~m~~	~~m~~	~~[26] 20.34~~	~~m~~	~~m~~
~~23~~	~~Subject~~	~~[26] 20.36~~	~~m~~	~~m~~	~~[26] 20.36~~	~~i~~	~~i~~
~~24~~	~~Supported~~	~~[26] 20.37~~	~~m~~	~~m~~	~~[26] 20.37~~	~~c6~~	~~c6~~
~~25~~	~~Timestamp~~	~~[26] 20.38~~	~~m~~	~~m~~	~~[26] 20.38~~	~~i~~	~~i~~
~~26~~	~~To~~	~~[26] 20.39~~	~~m~~	~~m~~	~~[26] 20.39~~	~~m~~	~~m~~
~~27~~	~~User-Agent~~	~~[26] 20.41~~	~~m~~	~~m~~	~~[26] 20.41~~	~~i~~	~~i~~
~~28~~	~~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.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.~~

~~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.~~

~~c9: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).~~

~~c10: IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.~~

~~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.163/6 - - INFO request~~

~~Table A.191: Supported message bodies within the INFO request~~

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

~~Prerequisite A.163/7 - - INFO response~~

~~Prerequisite: A.164/1 - - 100 (Trying)~~

~~Table A.192: Supported headers within the INFO response~~

~~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~~	~~Content-Length~~	~~[26] 20.14~~	~~m~~	~~m~~	~~[26] 20.14~~	~~m~~	~~m~~
~~3~~	~~Cseq~~	~~[26] 20.16~~	~~m~~	~~m~~	~~[26] 20.16~~	~~m~~	~~m~~
~~4~~	~~Date~~	~~[26] 20.17~~	~~m~~	~~m~~	~~[26] 20.17~~	~~c1~~	~~c1~~
~~5~~	~~From~~	~~[26] 20.20~~	~~m~~	~~m~~	~~[26] 20.20~~	~~m~~	~~m~~
~~6~~	~~To~~	~~[26] 20.39~~	~~m~~	~~m~~	~~[26] 20.39~~	~~m~~	~~m~~
~~7~~	~~Via~~	~~[26] 20.42~~	~~m~~	~~m~~	~~[26] 20.42~~	~~m~~	~~m~~
~~c1: IF A.162/9 THEN m ELSE i - - insertion of date in requests and responses.~~							

~~Prerequisite A.163/7 - - INFO response~~

~~Table A.193: Supported headers within the INFO 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~~
~~1A~~	~~Content-Disposition~~	~~[26] 20.11~~	~~m~~	~~m~~	~~[26] 20.11~~	~~i~~	~~c3~~
~~2~~	~~Content-Encoding~~	~~[26] 20.12~~	~~m~~	~~m~~	~~[26] 20.12~~	~~i~~	~~c3~~
~~2A~~	~~Content-Language~~	~~[26] 20.13~~	~~m~~	~~m~~	~~[26] 20.13~~	~~i~~	~~c3~~
~~3~~	~~Content-Length~~	~~[26] 20.14~~	~~m~~	~~m~~	~~[26] 20.14~~	~~m~~	~~m~~
~~4~~	~~Content-Type~~	~~[26] 20.15~~	~~m~~	~~m~~	~~[26] 20.15~~	~~i~~	~~c3~~
~~5~~	~~Cseq~~	~~[26] 20.16~~	~~m~~	~~m~~	~~[26] 20.16~~	~~m~~	~~m~~
~~6~~	~~Date~~	~~[26] 20.17~~	~~m~~	~~m~~	~~[26] 20.17~~	~~c1~~	~~c1~~
~~7~~	~~From~~	~~[26] 20.20~~	~~m~~	~~m~~	~~[26] 20.20~~	~~m~~	~~m~~
~~7A~~	~~MIME-Version~~	~~[26] 20.24~~	~~m~~	~~m~~	~~[26] 20.24~~	~~i~~	~~i~~
~~8~~	~~Organization~~	~~[26] 20.25~~	~~m~~	~~m~~	~~[26] 20.25~~	~~c2~~	~~c2~~
~~8A~~	~~Privacy~~	~~[33] 4.2~~	~~c4~~	~~c4~~	~~[33] 4.2~~	~~c5~~	~~c5~~
~~8B~~	~~Server~~	~~[26] 20.35~~	~~m~~	~~m~~	~~[26] 20.35~~	~~i~~	~~i~~
~~9~~	~~Timestamp~~	~~[26] 20.38~~	~~m~~	~~m~~	~~[26] 20.38~~	~~i~~	~~i~~
~~10~~	~~To~~	~~[26] 20.39~~	~~m~~	~~m~~	~~[26] 20.39~~	~~m~~	~~m~~
~~10A~~	~~User-Agent~~	~~[26] 20.41~~	~~m~~	~~m~~	~~[26] 20.41~~	~~i~~	~~i~~
~~11~~	~~Via~~	~~[26] 20.42~~	~~m~~	~~m~~	~~[26] 20.42~~	~~m~~	~~m~~
~~12~~	~~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.3/2 OR A.3/4 THEN m ELSE i - - P-CSCF or S-CSCF.~~
~~c4: IF A.162/31 THEN m ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).~~
~~c5: IF A.162/31D OR A.162/31G THEN m ELSE IF A.162/31C THEN i ELSE n/a - - application of the privacy option "header" or application of the privacy option "id" or passing on of the Privacy header transparently.~~

~~Prerequisite A.163/7 - - INFO response~~

~~Prerequisite: A.164/6 - - 2xx~~

~~Table A.194: Supported headers within the INFO 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~~
~~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~~
~~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.~~
~~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.163/7 - - INFO response~~

~~Prerequisite: A.164/8 OR A.164/9 OR A.164/10 OR A.164/11 OR A.164/12 - - 3xx~~

~~Table A.195: Supported headers within the INFO response~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Allow~~	~~[26] 20.5~~	~~m~~	~~m~~	~~[26] 20.5~~	~~i~~	~~i~~
~~1~~	~~Error-Info~~	~~[26] 20.18~~	~~m~~	~~m~~	~~[26] 20.18~~	~~i~~	~~i~~
~~3~~	~~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.163/7 - - INFO response~~

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

~~Table A.196: Supported headers within the INFO response~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Allow~~	~~[26] 20.5~~	~~m~~	~~m~~	~~[26] 20.5~~	~~i~~	~~i~~
~~1~~	~~Error-Info~~	~~[26] 2418~~	~~m~~	~~m~~	~~[26] 20.18~~	~~i~~	~~i~~
~~2~~	~~Proxy-Authenticate~~	~~[26] 20.27~~	~~m~~	~~m~~	~~[26] 20.27~~	~~m~~	~~m~~
~~3~~	~~Require~~	~~[26] 20.32~~	~~m~~	~~m~~	~~[26] 20.32~~	~~c2~~	~~c2~~
~~5~~	~~Supported~~	~~[26] 20.37~~	~~m~~	~~m~~	~~[26] 20.37~~	~~i~~	~~i~~
~~8~~	~~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.163/7 - - INFO 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.197: Supported headers within the INFO response~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Allow~~	~~[26] 20.5~~	~~m~~	~~m~~	~~[26] 20.5~~	~~i~~	~~i~~
~~1~~	~~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~~
~~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.~~							

~~Prerequisite A.163/7 - - INFO response~~

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

~~Table A.198: Supported headers within the INFO 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~~
~~4~~	~~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.~~						

~~Prerequisite A.163/7 - - INFO response~~

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

~~Table A.198A: Supported headers within the INFO 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] 2418~~	~~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.163/7 - - INFO response~~

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

~~Table A.199: Supported headers within the INFO response~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Accept~~	~~[26] 20.1~~	~~m~~	~~m~~	~~[26] 20.1~~	~~i~~	~~i~~
~~0B~~	~~Accept-Encoding~~	~~[26] 20.2~~	~~m~~	~~m~~	~~[26] 20.2~~	~~i~~	~~i~~
~~0C~~	~~Accept-Language~~	~~[26] 20.3~~	~~m~~	~~m~~	~~[26] 20.3~~	~~i~~	~~i~~
~~0D~~	~~Allow~~	~~[26] 20.5~~	~~m~~	~~m~~	~~[26] 20.5~~	~~i~~	~~i~~
~~1~~	~~Error-Info~~	~~[26] 20.18~~	~~m~~	~~m~~	~~[26] 20.18~~	~~i~~	~~i~~
~~3~~	~~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.163/7 - - INFO response~~

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

~~**Table A.200: Supported headers within the INFO response**~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Allow~~	~~[26] 20.5~~	~~m~~	~~m~~	~~[26] 20.5~~	~~i~~	~~i~~
~~1~~	~~Error-Info~~	~~[26] 20.18~~	~~m~~	~~m~~	~~[26] 20.18~~	~~i~~	~~i~~
~~3~~	~~Require~~	~~[26] 20.32~~	~~m~~	~~m~~	~~[26] 20.32~~	~~c2~~	~~c2~~
~~5~~	~~Supported~~	~~[26] 20.37~~	~~m~~	~~m~~	~~[26] 20.37~~	~~i~~	~~i~~
~~6~~	~~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.163/7 - - INFO response~~

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

~~**Table A.201: Supported headers within the INFO response**~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Allow~~	~~[26] 20.5~~	~~m~~	~~m~~	~~[26] 20.5~~	~~i~~	~~i~~
~~1~~	~~Error-Info~~	~~[26] 20.18~~	~~m~~	~~m~~	~~[26] 20.18~~	~~i~~	~~i~~
~~3~~	~~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.163/7 - - INFO response~~

~~Prerequisite: A.164/35 - - 485 (Ambiguous)~~

~~**Table A.202: Supported headers within the INFO response**~~

~~Item~~	~~Header~~	~~Sending~~			~~Receiving~~		
		~~Ref.~~	~~RFC status~~	~~Profile status~~	~~Ref.~~	~~RFC status~~	~~Profile status~~
~~0A~~	~~Allow~~	~~[26] 20.5~~	~~m~~	~~m~~	~~[26] 20.5~~	~~i~~	~~i~~
~~1~~	~~Error-Info~~	~~[26] 20.18~~	~~m~~	~~m~~	~~[26] 20.18~~	~~i~~	~~i~~
~~3~~	~~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.163/7 - - INFO response~~

~~**Table A.203: Supported message bodies within the INFO response**~~

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

3GPP TSG-CN1 Meeting #30 ***Tdoc N1-030~~9~~840***
San Diego, California, USA, 19 – 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘	**24.229**	**CR**	**377**	⌘ **rev**	**1**	⌘	Current version:	**5.4.0**	⌘

*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:	⌘	Use of the QoS parameter ‘signalling information’ for a signalling PDP context		
Source:	⌘	Ericsson, Nokia		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	20/05/2003
Category:	⌘	**F** *Use one of the following categories:* ***F** (correction)* ***A** (corresponds to a correction in an earlier release)* ***B** (addition of feature),* ***C** (functional modification of feature)* ***D** (editorial modification)* Detailed explanations of the above categories can be found in 3GPP TR 21.900.	***Release:*** ⌘	Rel-5 *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:	⌘	Use of the QoS parameter ‘signalling information’ for a signalling PDP context
Summary of change:	⌘	The enhanced QoS for ‘signalling indication’ shall be used when a dedicated PDP context for IMS signalling is used. The following changes are proposed: ▪ The QoS Signalling Indication and the IMS signalling flag are independant. ▪ The Note 1 is removed. The CR aligns with stage-2 changes approved in SA2#31. A new parameter, ‘Signalling Indication’, has been introduced in the QoS IE, see stage 2 specifications; S2-031527 (CR to 23.228), S2-031482 (CR to 23.207). For deletion of NOTE1, note also the agreed text within 23.228: ”The IM CN Subsystem Signalling flag is used to indicate the dedicated signalling PDP context for IMS signalling. <u>If the network operator does not support a dedicated signalling PDP context</u> or the UE does not include the IM CN Subsystem Signalling flag, <u>the network will consider the PDP context as a general purpose PDP context</u>.”
Consequences if not approved:	⌘	The handling of the QoS parameter ‘signalling indication’ is not according to the stage 2 for IMS.

Clauses affected:	⌘	2, 9.2.1	
		Y	**N**

Other specs	⌘	**X**		Other core specifications	⌘	24.008 (CR no. 759, 760) 27.060 (CR no. 084) 29.061 (CR no. 087)
affected:			**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 change ****

2 References

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

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

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

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

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

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

[4A] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[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".

[9A] 3GPP TS 25.331: "Radio Resource Control (RRC); Protocol Specification".

[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".

[20A] RFC 2401 (November 1998): "Security Architecture for the Internet Protocol".

[21] RFC 2617 (June 1999): "HTTP Authentication: Basic and Digest Access Authentication".

[22] RFC 2806 (April 2000): "URLs for Telephone Calls".

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

[24] RFC 2916 (September 2000): "E.164 number and DNS".

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

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

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

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

[29] RFC 3311 (September 2002): "The Session Initiation Protocol (SIP) UPDATE method".

[30] RFC 3312 (October 2002): "Integration of resource management and Session Initiation Protocol (SIP)".

[31] RFC 3313 (January 2003): "Private Session Initiation Protocol (SIP) Extensions for Media Authorization".

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

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

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

[35] RFC 3327 (December 2002): "Session Initiation Protocol Extension Header Field 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] RFC 3420 (November 2002): "Internet Media Type message/sipfrag".

[38] draft-ietf-sip-scvrtdisco-01 (August 2002): "Session Initiation Protocol Extension Header Field for Service Route Discovery During Registration".

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] RFC 3485 (February 2003): "The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) static dictionary for Signaling Compression (SigComp)".

[43] draft-ietf-sipping-reg-event-00 (October 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] Void.

[45] Void.

[46] Void.

[47] Void.

[48] RFC 3329 (January 2003): "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[49] RFC 3310 (September 2002): "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[50] RFC 3428 (December 2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[51] Void.

[52] RFC 3455 (January 2003): "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)".

[53] RFC 3388 (December 2002): "Grouping of Media Lines in Session Description Protocol".

[54] draft-ietf-mmusic-reservation-flows-01.txt (October 2002): "Mapping of Media Streams to Resource Reservation Flows".

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

[55] RFC 3486 (February 2003): "Compressing the Session Initiation Protocol (SIP)"

**** 2nd change ****

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 as described in 3GPP TS 29.061 [11]. The UE can also set the Signalling Indication attribute within the QoS IE;

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 can also set the Signalling Indication attribute within the QoS IE.

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. Upon successful signalling PDP context establishment the UE receives an indication from GGSN in the form of IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE. If the flag is not received, the UE shall consider the PDP context as a general-purpose PDP context.

~~NOTE 1: Indication of successful signalling PDP context establishment is needed for the case when the GGSN does not receive the IM CN Subsystem Signalling Flag from the SGSN. Consequently, it acknowledges a request for activating a PDP Context without an IM CN Subsystem Signalling Flag. The UE will then regard it as a general-purpose PDP context instead of as a dedicated PDP context for SIP signalling as initially requested by the UE.~~

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

The UE can indicate a request for prioritised handling over the radio interface by setting the Signalling Indication attribute (see 3GPP TS 23.107 [4A]). The general QoS negotiation mechanism and the encoding of the Signalling Indication attribute within the QoS IE are described in 3GPP TS 24.008 [8].

NOTE~~ 2~~: 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 stream 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~~The encoding of ~~how~~ the request and response for IPv6 address(es) for DNS server(s) and list of P-CSCF address(es) within~~are carried in~~ the Protocol Configuration Options IE is ~~provided~~ described 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 established as a result of SIP signalling according to the 3GPP TS 24.008 [8].

3GPP TSG-CN1 Meeting #30 **Tdoc N1-030919~~621~~**
San Diego, California, USA, 19 – 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **378** ⌘**rev** **2** ⌘ Current version: **5.4.0** ⌘

*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: ⌘	Deregistration of a PUID (not the last one)		
Source: ⌘	Orange		
Work item code: ⌘	IMS-CCR	***Date:*** ⌘	05/05/2003
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: ⌘	When a public user identity is deregistered and there is at least one remaining public user identity registered, the currently active sessions established with the public user identity being deregistered are not released. This leads to the situation where a user has a public user identity deregistered (and at least one public user identity registered) but has still an established session with this deregistered public user identity.
Summary of change: ⌘	It is added that in the case a public user identity is deregistered, all sessions established with this public user identity or with an implicilty registered public user identity shall be released.
Consequences if not approved: ⌘	It may happen that a user has a public user identity deregistered (and at least one public user identity registered) but has still an established session with this deregistered public user identity

Clauses affected: ⌘	5.1.1.6, 5.1.1.7, 5.4.1.4, 5.4.1.5				
	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.

5.1.1.6 Mobile-initiated deregistration

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

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

Prior to sending a REGISTER request for deregistration, the UE shall release all dialogs related to the public user identity that is going to be deregistered or to one of the implicitly registered public user identities.

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

a) the Authorization header, with the username field, set to the value of the private user identity;

b) the From header set to the SIP URI that contains the public user identity to be deregistered;

c) the To header set to the SIP URI that contains the public user identity to be deregistered;

d) the Contact header set to either the value of "*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected port value bound to the security association;

e) the Expires header, or the expires parameter of the Contact header, set to the value of zero, appropriate to the deregistration requirements of the user;

f) a Request-URI set to the SIP URI of the domain name of the home network; and

g) a P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

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.

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

~~The UE shall release all dialogs prior to deregistering the last registered public user identity.~~

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

If all public user identities are deregistered and the security association is removed, then the UE shall consider subscription to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

NOTE: When the UE has received the 200 (OK) for the REGISTER request of the last registered public user identity, the UE removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY contaning the deregistration event) will not reach the UE.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxNEXT CHANGExxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

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 5.1.1.3, including one or more <registration> element(s) with the state attribute set to "terminated" and the event attribute set to "rejected" or "deactivated", the UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the reregistration procedure as described in subclause 5.1.1.4. In case of a "rejected" event attribute, the UE shall release all dialogs related to those public user identities.

Upon receipt of a NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header contains the value of "terminated", the UE shall remove the security associations towards the P-CSCF after the server transaction (as defined in RFC 3261 [26]) pertaining to the NOTIFY request terminates.

NOTE 1: If the security association towards the P-CSCF is removed, then the UE considers the subscription to the registration event package terminated (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero, or a NOTIFY request was received with Subscription-State header containing the value of "terminated").

NOTE 2: When the P-CSCF has removed the security association established between the P-CSCF and the UE, further SIP signalling (e.g. the NOTIFY contaning the deregistration event) will not reach the UE.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxNEXT CHANGExxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

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;
- release each multimedia session which was initiated with the public user identity found in the P-Asserted-Identity header field or with one of the implicitly registered public used identities by applying the steps listed in subclause 5.4.5.1.2;
- deregister the public user identity found in the To header field together with the implicitly registered public user identities;
- send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event; and
- if this is a deregistration request for the last registered public user identity and there are still active multimedia sessions associated with this user, release each multimedia session belonging to the served user by applying the steps listed in subclause 5.4.5.1.2.

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 all public user identities of the UE are deregistered, then the S-CSCF may consider the UE and P-CSCF subscriptions to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

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.

xxxxxxxxxxxxxxxxxxxxxxxxxxxxNEXT CHANGExxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

5.4.1.5 Network-initiated deregistration

Prior to initiating the network-initiated deregistration for the last registered public user identity while there are still active multimedia sessions belonging to this user, the S-CSCF shall release all multimedia sessions belonging to this user as described in subclause 5.4.5.1.

When a network-initiated deregistration event occurs for one or more public user identity, the S-CSCF shall send a NOTIFY request to the UE on the dialog which was generated by the UE subscribing to the registration event package. When the S-CSCF receives a final response to the NOTIFY request or upon a timeout, the S-CSCF shall release all remaining dialogs related to the public user identity being deregistered and shall generate a NOTIFY request on all remaining dialogs which have been established due to subscription to the reg event package of that user. For each NOTIFY request, the S-CSCF shall:

- set the Request-URI and Route header to the saved route information during subscription;
- set the Event header to the "reg" value;
- in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;
- set the aor attribute within each <registration> element to one public user identity:
  - set the <contact> sub-element of each <registration> element to the contact address provided by the UE;
  - if the public user identity:
    - has been deregistered then:
      - set the state attribute within the <registration> element to "terminated";
      - set the state attribute within the <contact> element to "terminated"; and
      - set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or
    - has been kept registered then:
      - set the state attribute within the <registration> element to "active"; and
      - set the state attribute within the <contact> element to "active".

When sending a final NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered), the S-CSCF shall also terminate the subscription to the registration event package by setting the Subscription-State header to the value of "terminated".

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

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.

3GPP TSG-CN1 Meeting #30 **Tdoc N1-030920~~622~~**
San Diego, California, USA, 19 – 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘	**24.229**	**CR**	**379**	⌘ **rev**	**2**	⌘	Current version:	**5.4.0** ⌘

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: ⌘	'Last registered public user identity' terminology change		
Source: ⌘	Orange		
Work item code: ⌘	IMS-CCR	***Date:*** ⌘	05/05/2003
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 wording 'last registered public user identity' is misleading as two different meanings can be understand:

- public user identity that has been registered at the latest registration
- the only public user identity remaining registered (the user has only one public user identity currently registered, associated with the implicitly registered public user identities).

The second understanding is the correct one.

Summary of change: ⌘ The wording 'last registered public user identity' is changed into 'only public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered)' at each occurrence with this specification

Consequences if not approved: ⌘ There will be wrong implementations if wrong understanding is considered.

Clauses affected: ⌘ 5.1.1.6, 5.2.5.1, 5.4.1.4, 5.4.1.5, 5.4.5.1.2A

	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.

5.1.1.6 Mobile-initiated deregistration

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

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

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

a) the Authorization header, with the username field, set to the value of the private user identity;

b) the From header set to the SIP URI that contains the public user identity to be deregistered;

c) the To header set to the SIP URI that contains the public user identity to be deregistered;

d) the Contact header set to either the value of "*" or SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN and protected port value bound to the security association;

e) the Expires header, or the expires parameter of the Contact header, set to the value of zero, appropriate to the deregistration requirements of the user;

f) a Request-URI set to the SIP URI of the domain name of the home network; and

g) a P-Access-Network-Info header that contains information concerning the access network technology and, if applicable, the cell ID (see subclause 7.2A.4).

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.

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

The UE shall release all dialogs prior to deregistering the last registered public user identity.

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

If all public user identities are deregistered and the security association is removed, then the UE shall consider subscription to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

NOTE: When the UE has received the 200 (OK) for the REGISTER request of the only ~~last registered~~ public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered), the UE removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY contaning the deregistration event) will not reach the UE.

Next change*******************************

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, if the subscription to the reg event package for that user is still alive, terminate the subscription to the reg event package for that user by sending a SUBSCRIBE request with an Expires header containing a value of zero. The P-CSCF shall also remove the security associations towards that user after the server transaction (as defined in RFC 3261 [26]) pertaining to this deregistration terminates.

NOTE 1: 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.

NOTE 2: When the P-CSCF has sent the 200 (OK) for the REGISTER request of the only ~~last registered~~ public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered), the P-CSCF removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY contaning the deregistration event) will not reach the UE.

Next change****************************

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;
- 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
- if this is a deregistration request for the only ~~last registered~~ public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered) and there are still active multimedia sessions associated with this user, release each multimedia session belonging to the served user by applying the steps listed in subclause 5.4.5.1.2.

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 all public user identities of the UE are deregistered, then the S-CSCF may consider the UE and P-CSCF subscriptions to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero).

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.

Next change****************************

5.4.1.5 Network-initiated deregistration

Prior to initiating the network-initiated deregistration for the only ~~last registered~~ public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered) while there are still active multimedia sessions belonging to this user, the S-CSCF shall release all multimedia sessions belonging to this user as described in subclause 5.4.5.1.

When a network-initiated deregistration event occurs for one or more public user identity, the S-CSCF shall send a NOTIFY request to the UE on the dialog which was generated by the UE subscribing to the registration event package. When the S-CSCF receives a final response to the NOTIFY request or upon a timeout, the S-CSCF shall generate a NOTIFY request on all remaining dialogs which have been established due to subscription to the reg event package of that user. For each NOTIFY request, the S-CSCF shall:

- set the Request-URI and Route header to the saved route information during subscription;
- set the Event header to the "reg" value;
- in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;
- set the aor attribute within each <registration> element to one public user identity:
  - set the <contact> sub-element of each <registration> element to the contact address provided by the UE;
  - if the public user identity:
    - has been deregistered then:
      - set the state attribute within the <registration> element to "terminated";
      - set the state attribute within the <contact> element to "terminated"; and
      - set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or
    - has been kept registered then:
      - set the state attribute within the <registration> element to "active"; and
      - set the state attribute within the <contact> element to "active".

When sending a final NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered), the S-CSCF shall also terminate the subscription to the registration event package by setting the Subscription-State header to the value of "terminated".

The S-CSCF shall only include the non-barred public user identities in the NOTIFY request.

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.

Next change*******************************

5.4.5.1.2A Release of the existing dialogs due to registration expiration

When the registration lifetime of the only ~~last registered~~ public user identity currently registered with its associated set of implicitly registered public user identities (i.e. no other is registered) expires while there are still active multimedia sessions belonging to the served user, the S-CSCF shall release each multimedia session belonging to the served user by applying the steps listed in the subclause 5.4.5.1.2.

3GPP TSG-CN1 Meeting #30 **Tdoc N1-030881**
San Diego, California, USA, 19 – 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229 CR 380** ⌘**rev 1** ⌘ Current version: **5.4.0** ⌘

*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:	⌘	Check Integrity Protection for P-Access-Network-Info header		
Source:	⌘	3		
Work item code:	⌘	IMS-CCR	***Date:*** ⌘	08/05/2003
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:	⌘	Rev1 -------- After review of revision 1 it was noted that there was a need to highlight the behaviour, but that this should be done in section 5.4.1.7. The 3rd party text should be moved from the general section 5.4.1.1 to 5.4.1.7. The need to have the proposed added condition about the REGISTER being integrity protected is not needed as this is a prerequisite for 3rd party REGISTER to AS anyway. Changes modified to reflect this. Rev0 (N1-030635) ------ The P-Access-Network-Info header should only be included if a security association exists (as stated in 5.1.1.2 bullet i). However the specification does not state that this is checked at the S-CSCF in the approriate section.
Summary of change:	⌘	Moved statements regarding 3rd party REGISTER to AS from general section (5.4.1.1) to the section dealing with third party registration (5.4.1.7).
Consequences if not approved:	⌘	There may be ambiguity regarding the inclusiosn of P-Access-Network-Info header as highlighted by the initial proposal

Clauses affected:	⌘	5.4.1.1, 5.4.1.7				
		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.

5.4.1.1 Introduction

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

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

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

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

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

5.4.1.7 Notification of Application Servers about registration status

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

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, 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 the S-CSCF shall include 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, which shall contain the values received from the HSS if the message is forwarded within the S-CSCF home network.