3GPP TSG CN Plenary Meeting #20   NP-030281
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 7**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **10** 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	426		F	Rel-5	P-CSCF procedure tidyup	5.4.0	5.5.0	N1-30	N1-030755
24.229	427		F	Rel-5	I-CSCF procedure tidyup	5.4.0	5.5.0	N1-30	N1-030756
24.229	428		F	Rel-5	S-CSCF procedure tidyup	5.4.0	5.5.0	N1-30	N1-030757
24.229	429		F	Rel-5	BGCF procedure tidyup	5.4.0	5.5.0	N1-30	N1-030758
24.229	430		F	Rel-5	AS procedure tidyup	5.4.0	5.5.0	N1-30	N1-030759
24.229	431		F	Rel-5	MRFC procedure tidyup	5.4.0	5.5.0	N1-30	N1-030760
24.229	434	1	F	Rel-5	SDP procedure tidyup	5.4.0	5.5.0	N1-30	N1-030852
24.229	438	2	F	Rel-5	Profile Tables – Further Corrections	5.4.0	5.5.0	N1-30	N1-030935
24.229	439	3	F	Rel-5	AS's subscription for the registration state event package	5.4.0	5.5.0	N1-30	N1-030940
24.229	440		F	Rel-5	Temporary Public User Identity in re- and de-REGISTER requests	5.4.0	5.5.0	N1-30	N1-030792

CR-Form-v7

CHANGE REQUEST

| ⌘ | **24.229** | CR | **426** | ⌘**rev** | **-** | ⌘ | 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 **X**

Title: ⌘	P-CSCF procedure tidyup	
Source: ⌘	Lucent Technologies	
Work item code:⌘	IMS-CCR	**Date:** ⌘ 01/05/2003
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: ⌘	1. Subclause 5.2.2, 1st paragraph, item 5, curly quotes converted to smart quotes in accordance with drafting rules.
	2. Subclause 5.2.2, 1st paragraph, item 6, 1st subitem, "error" code changed to "response" to align with RFC 3261 terminology. insertion of "the P-CSCF shall" to make the requirement clear in 3rd sentence.
	3. Subclause 5.2.2, 3rd paragraph, item 4, insertion of "header" after P-Asserted-Identity in order to make clear that it is a header. Subclause 5.2.2, last paragraph and note is not requirements relating to registration, but to existing dialogs. Therefore it belongs in a different clause. Moreover, the same situation in the S-CSCF has been covered in text related to release of dialogs. Therefore, and in alignment with the procedures for the S-CSCF, it is proposed that this text is moved (unchanged) to a new clause 5.2.8.1.4.
	4. Subclause 5.2.5.1, note 2, insertion of word "response" after "200 (OK)". "request" added after NOTIFY and typo corrected in following word.
	5. Subclause 5.2.5.2, note, "request" added after NOTIFY and typo corrected in following word.
	6. Subclause 5.2.10. Various parts of this subclause are written in the passive sense, and some modifications are proposed to change it to the active sense.

Summary of change:⌘	See above

Consequences if ⌘ **not approved:**	Unclear specification

Clauses affected: ⌘	5.2.2, 5.2.5.1, 5.2.5.2, 5.2.8.1.4 (new), 5.2.10

	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.

PROPOSED CHANGE

5.2.2 Registration

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

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

   - the SIP URL identifying the P-CSCF;

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

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

3) for the initial REGISTER request for a public user identity create a new, globally unique value for icid, save it locally and insert it into the icid parameter of the P-Charging-Vector header;

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

5) in case the REGISTER request was received without integrity protection, then check the existence of the Security-Client header. If the header is present, then remove and store it. The P-CSCF shall remove the '"sec-agree'" item from the Require header, and the header itself if this is the only entry. If the header is not present, then the P-CSCF shall return a suitable 4xx response;

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

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

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

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

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

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

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

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

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

3) set up the security association with a temporary lifetime between the UE and the P-CSCF for the user identified with the private user identity. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]. The P-CSCF shall set the SIP level lifetime of the security association to be long enough to permit the UE to finalize the

registration procedure (bigger than 64*T1). The P-CSCF shall set the IPSec level lifetime of the security association to the maximum.

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

1) save the list of Service-Route headers preserving the order. The P-CSCF shall store this list during the entire registration period of the respective public user identity. The P-CSCF shall use this list to validate the routeing information in the requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing list of Service-Route headers with the new list;

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

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

4) store the default public user identity for use with procedures for the P-Asserted-Identity header. The default public user identity is the first on the list of URIs present in the P-Associated-URI header;

NOTE 1: There may be more then one default public user identities stored in the P-CSCF, as the result of the multiple registrations of public user identities.

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

6) update the SIP level lifetime of the security association with the value found in the Expires header;

7) protect the response within the same security association to that in which the associated request was protected;

8) delete all earlier security associations and related keys it may have towards the UE, when a message protected within the newly set up security association is received; and

9) delete the new security associations that it was trying to establish with the UE, in case the P-CSCF receives a message from the UE protected with the old security association.

NOTE 2: The P-CSCF will maintain two Route header lists. The first Route header list - created during the registration procedure - is used only to validate the routeing information in the initial requests that originate from the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

The P-CSCF shall delete any security association from the IPSec database when their SIP level lifetime expires. ~~If there are still active dialogs associated with the user after the security associations were deleted, the P-CSCF shall discard all information pertaining to these dialogs without performing any further SIP transactions with the peer entities of the P-CSCF.~~

NOTE 3: ~~At the same time, the P-CSCF will also indicate via the Go interface that all resources associated with these dialogs should be released.~~

PROPOSED 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) response for the REGISTER request of the last registered public user identity, the P-CSCF removes the security association established between the P-CSCF and the UE. Therefore further SIP signalling (e.g. the NOTIFY request containing contaning the deregistration event) will not reach the UE.

PROPOSED CHANGE

5.2.5.2 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 5.2.3, including one or more <registration> element(s) with the state attribute set to "terminated" the P-CSCF shall remove all stored information for these 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), the P-CSCF shall remove the security associations towards the UE.

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

PROPOSED CHANGE

5.2.8.1.4 Release of the existing dialogs due to registration expiration and deletion of the security association

If there are still active dialogs associated with the user after the security associations were deleted, the P-CSCF shall discard all information pertaining to these dialogs without performing any further SIP transactions with the peer entities of the P-CSCF.

NOTE: At the same time, the P-CSCF will also indicate via the Go interface that all resources associated with these dialogs should be released.

PROPOSED CHANGE

5.2.10 Emergency service

The P-CSCF shall store a configurable list of local emergency numbers and emergency URLs, i.e. those used for emergency services by the operator to which the P-CSCF belongs to. In addition to that, the P-CSCF shall store a configurable list of roaming partners' emergency numbers and emergency URLs associated with MCC and MNC codes.

NOTE: Certain SIP URLs may be classified as emergency URLs in all networks.

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

In order to determine whether the INVITE request is destined for an emergency centre in the roaming country (i.e. the list of roaming partners' are inspected), the P-CSCF shall compare the MCC and the MNC fields in the received in the P-Access-Network-Info header of the INVITE request against its own MCC and MNC codes.

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

The P-CSCF shall include in the The 3GPP IMS XML body:

a)   shall contain an <alternative-service> element, that indicates set to the parameters of the alternative service;.

b)   The a <type> child element, shall be set to "emergency" to indicate that it was an emergency call; and

c)   a . An operator configurable <reason> child element, set to shall be included with a reason phrasean operator configurable reason.

CR-Form-v7

CHANGE REQUEST

| | ⌘ | **24.229** CR **427** | ⌘**rev** | **-** | ⌘ | 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 **X**

Title:	⌘	I-CSCF procedure tidyup
Source:	⌘	Lucent Technologies
Work item code:⌘	IMS-CCR	***Date:*** ⌘ 01/05/2003
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 word further in both the title of subclause 5.3.2, and in the text of 5.3.2.1 conveys no additional meaning, and is not defined with a specific meaning in relation to initial requests, and therefore it is proposed to be deleted.
		• In subclause 5.3.2.1, 6th paragraph, the text is currently written in the passive sense. It is proposed to rewrite this in the active sense.
		• In subclause 5.3.3.1, 2nd paragraph and 3rd paragraph contains text in the passive sense, and would be better written in the active. Such a proposal is made.
		• There are a number of instances in the text were "initial request" really means "initial request for a dialog or standalone transaction". Without that expansion, the understanding that it also applies to standalone transactions could be lost, and therefore the text is expanded.

Summary of change: ⌘		See above
Consequences if not approved:	⌘	Unclear specification

Clauses affected:	⌘	5.3.2, 5.3.2.1, 5.3.3.1,

	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.

PROPOSED CHANGE

5.3.2 ~~Further i~~Initial requests

5.3.2.1 Normal procedures

The I-CSCF may behave as a stateful proxy for ~~further~~ initial requests.

When the I-CSCF receives an initial request for a dialog or standalone transaction, that does not contain a Route header, the I-CSCF shall start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [14] for the called user, indicated in the Request-URI. Prior to performing the user location query procedure to the HSS, the I-CSCF decides which HSS to query, possibly as a result of a query to the Subscription Locator Functional (SLF) entity as specified in 3GPP TS 29.228 [14].

Upon successful user location query, when the response contains the URL of the assigned S-CSCF, the I-CSCF shall:

1) insert the URL received from the HSS as the topmost Route header;

2) 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. If no icid parameter was found, then create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header;

3) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and

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

Upon successful user location query, when the response contains information about the required S-CSCF capabilities, the I-CSCF shall:

1) select a S-CSCF according to the method described in 3GPP TS 29.228 [14];

2) insert the URL of the selected S-CSCF as the topmost Route header field value;

3) execute the procedure described in step 2 and 3 in the above paragraph (upon successful user location query, when the response contains the URL of the assigned S-CSCF); and

4) forward the request to the selected S-CSCF.

Upon an unsuccessful user location query when the response from the HSS indicates that the user does not exist, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) or 604 (Does not exist anywhere) in the case the user is not a user of the home network.

Upon an unsuccessful user location query when the response from the HSS indicates that the user is not registered and no services are provided for such a user, the I-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) if the user is recognized as a valid user, but is not registered at the moment and it does not have services for unregistered users.

When the I-CSCF receives an initial request for a dialog or standalone transaction, that contains a single Route header pointing to itself, the I-CSCF shall determine from the entry in the Route header whether it needs to do HSS query or hiding. In case HSS query is needed, then the I-CSCF shall perform the procedures described for the case when there is no Route header present ~~shall be performed~~. If the I-CSCF determines that hiding must be performed, then the THIG functionality in I-CSCF received an outgoing initial request for which topology hiding has to be applied, and the I-CSCF shall:

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

2) perform the procedures described in subclause 5.3.3; and

3) route the request based on the Request-URI header field.

When the I-CSCF receives an initial request for a dialog or standalone transaction containing more than one Route header, the I-CSCF shall:

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

2) apply the procedures as described in subclause 5.3.3; and

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

NOTE: In accordance with SIP the I-CSCF can add its own routeable SIP URL to the top of the Record-Route header to any request, independently of whether it is an initial request, or whether topology hiding is performed. The P-CSCF will ignore any Record-Route header that is not in the initial request of a dialog.

When the I-CSCF receives a response to an initial request (e.g. 183 or 2xx), the I-CSCF shall store the values from the P-Charging-Function-Addresses header, if present. If the next hop is outside of the current network, then the I-CSCF shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

PROPOSED CHANGE

5.3.3.1   General

The following procedures shall only be applied if topology hiding is required by the network. The network requiring topology hiding is called the hiding network.

NOTE 1: Requests and responses are handled independently therefore no state information is needed for that purpose within an I-CSCF(THIG).

The I-CSCF(THIG) shall apply topology hiding to all ~~All~~ headers which reveal topology information, such as Via, Route, Record-Route, Service-Route~~, shall be subject to topology hiding~~.

Upon receiving an incoming REGISTER request for which topology hiding has to be applied and which includes a Path header, the I-CSCF(THIG) shall add the routeable SIP URL of an I-CSCF(THIG) to the top of the Path header. The I-CSCF(THIG) may include in the inserted SIP URL ~~may include~~ an indicator that identifies the direction of subsequent requests received by the I-CSCF i.e., from the S-CSCF towards the P-CSCF, to identify the mobile-terminating case. The I-CSCF(THIG) may encode this ~~This~~ indicator ~~may be encoded~~ in different ways, such as, e.g., a unique parameter in the URL, a character string in the username part of the URL, or a dedicated port number in the URL.

NOTE 2: Any subsequent request that includes the direction indicator (in the Route header) or arrives at the dedicated port number, indicates that the request was sent by the S-CSCF towards the P-CSCF.

Upon receiving an incoming initial request for which topology hiding has to be applied and which includes a Record-Route header, the I-CSCF(THIG) shall add its own routeable SIP URL to the top of the Record-Route header.

Upon receiving an outgoing initial request for which topology hiding has to be applied and which includes P-Charging-Function-Addresses header, the I-CSCF(THIG) shall remove the P-Charging-Function-Addresses header prior to forwarding the message.

CR-Form-v7

CHANGE REQUEST

⌘	**24.229** CR **428**	⌘**rev**	**-**	⌘	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 **X**

Title:	⌘	S-CSCF procedure tidyup		
Source:	⌘	Lucent Technologies		
Work item code: ⌘	IMS-CCR		*Date:* ⌘	01/05/2003
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: ⌘	1. Subclause 5.4.1.1, 5th paragraph, minor revisions made for clarity. 2. Subclause 5.4.1.2.3, addition of word "response" to various status code values where it is missing. 3. Subclause 5.4.1.5, 2nd and 3rd paragraphs refers to the registration event package. The correct name for the package is the reg event package and this is what is used elsewhere in the document. It is changed to make it consistent. 4. Subclause 5.4.1.5, 2nd paragraph, the only way to determine the level of indent is by the style used (B1, B2, B3 etc.). As this could be lost at some future editing process, it is proposed that the items are numbered, using different numbering for different levels of indentation. 5. Subclause 5.4.2.1.1, 1st paragraph, item 1, "this" changed to "the" to enable the text to read correctly. 6. Subclause 5.4.2.1.1, 2nd paragraph, item 2, format of text relating to headers changed to correspond to format used in subclause 5.1.1.4, etc. 7. Subclause 5.4.3.2, 1st paragraph, item 4, some minor rewording to match the introductory text for the items (the text of the item should continue from the introductory text). 8. Subclause 5.4.3.2, 3rd paragraph, the contents of the Record-Route header should only be saved on a 1xx or 2xx response. Any other response does not result in a dialog that needs to be cleared. The text is therefore modified accordingly. 9. Subclause 5.4.3.2, 5th paragraph, the contents of the Record-Route header should only be saved on a 1xx or 2xx response. Any other response does not result in a dialog that needs to be cleared. The text is therefore modified accordingly. 10. Subclause 5.4.3.3, 3rd paragraph, the contents of the Record-Route header should only be saved on a 1xx or 2xx response. Any other response does not result in a dialog that needs to be cleared. The text is therefore

11. Subclause 5.4.3.3, 7th paragraph, the contents of the Record-Route header should only be saved on a 1xx or 2xx response. Any other response does not result in a dialog that needs to be cleared. The text is therefore modified accordingly.

12. Subclause 5.4.4.2.1, last paragraph. Inclusion of the P-Charging-Vector and P-Charging-Functional-Addresses header into ACK and CANCEL is precluded by RFC 3455, and therefore this restriction also needs to be written into this paragraph, where such inclusion is currently allowed. The text is therefore modified accordingly.

13. Subclause 5.4.4.2.2, contains some extra words that presumably should have been deleted based on a change in a previous CR. They are deleted.

14. Subclause 5.4.4.2.2, last paragraph. Inclusion of the P-Charging-Vector and P-Charging-Functional-Addresses header into ACK and CANCEL is precluded by RFC 3455, and therefore this restriction also needs to be written into this paragraph, where such inclusion is currently allowed. The text is therefore modified accordingly.

Summary of change: ⌘	See above

Consequences if not approved: ⌘	Unclear specification

Clauses affected: ⌘	5.4.1.1, 5.4.1.2.3, 5.4.1.5, 5.4.2.1.1, 5.4.3.2, 5.4.3.3, 5.4.4.2.1, 5.4.4.2.2

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

Other comments: ⌘	

How to create CRs using this form:

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

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

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

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

PROPOSED CHANGE

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 sent towards the 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.

PROPOSED CHANGE

5.4.1.2.3   Abnormal cases

The S-CSCF need not challenge an unprotected REGISTER request for a private user identity that already has a registration in process, but instead return a 500 (Server Internal Error) response. The response shall contain a Retry-After header with a value indicating a time the UE shall wait before resending the request.

In the case that the authentication response (RES) from the UE does not match with XRES and the request was correctly integrity protected (it is indicated by the P-CSCF), or the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), and the authentication response was triggered by an initial registration or a UE initiated reauthentication, the S-CSCF shall either:

-    start a network initiated re-authentication procedure as defined in subclause 5.4.1.6; or

-    send a further challenge in a 401 (Unauthorized) response to the UE.

In the case that the authentication response (RES) from the UE does not match with XRES and the request was correctly integrity protected (it is indicated by the P-CSCF), or the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), and the authentication response was triggered by a network initiated reauthentication the S-CSCF shall either:

-    attempt a further authentication challenge; or

-    deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the REGISTER request from the UE containing an authentication response indicates that the authentication challenge was invalid and with no RES or AUTS parameter, the S-CSCF shall:

-    respond with the relevant 4xx response (e.g. a 401 (Unauthorized) response to initiate a further authentication attempt, or 403 (Forbidden) response if the authentication attempt is to be abandoned).

In the case that the REGISTER request from the UE containing an authentication response indicates that the authentication challenge was invalid but contains the AUTS parameter, the S-CSCF will fetch new authentication vectors from the HSS, including AUTS and RAND in the request to indicate a resynchronisation. On receipt of these vectors from the HSS, the S-CSCF shall:

- send a 401 (Unauthorized) response to initiate a further authentication attempt, using these new vectors.

In the case that the expiration timer from the UE is too short to be accepted by the S-CSCF, the S-CSCF shall:

- reject the REGISTER request with a 423 (Interval Too Brief) response, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

On receiving a failure response to one of the third-party REGISTER requests, the S-CSCF may initiate network-initiated deregistration procedure based on the information in the Filter Criteria. If the Filter Criteria does not contain instruction to the S-CSCF regarding the failure of the contact to the Application Server, the S-CSCF shall not initiate network-initiated deregistration procedure.

In the case that the REGISTER request from the UE contains more than one SIP URIs as Contact header entries, the S-CSCF shall only store the entry with the highest "q" value and include it in the 200 (OK) response.

PROPOSED CHANGE

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 reg 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:

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

2) set the Event header to the "reg" value;

3) 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;

4) set the aor attribute within each <registration> element to one public user identity:

    a) set the <contact> sub-element of each <registration> element to the contact address provided by the UE;

    b) if the public user identity:

        i) 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

        ii) 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 reg 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.

PROPOSED CHANGE

5.4.2.1.1 Subscription to the event providing registration state

When an incoming SUBSCRIBE request addressed to S-CSCF arrives containing the Event header with the reg event package, the S-CSCF shall:

1) check if, based on the local policy, the request was generated by a subscriber who is authorised to subscribe to ~~this~~ the registration state of this particular user. The authorized subscribers include:

   - all public user identities this particular user owns, that the S-CSCF is aware of, and which are not-barred;

   - all the entities identified by the Path header (i.e. the P-CSCF to which this user is attached to); and

   - all the ASs not belonging to third-party providers.

2) generate a 2xx response acknowledging the SUBSCRIBE request and indicating that the authorised subscription was successful as described in draft-ietf-sipping-reg-event-00 [43]. ~~Furthermore, the response~~ The S-CSCF shall ~~include~~populate the header fields as follows:

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

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

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

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

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

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 1xx or 2xx response to the initial request for a dialog, it the S-CSCF shall save the necessary Record-Route header fields and the Contact header from the response in order to release the dialog if needed.

When the S-CSCF receives from the served user a 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 request in order to release the dialog when needed;

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

When the S-CSCF receives a <u>1xx or 2xx</u> response to the target refresh request for a dialog, it shall save the necessary Record-Route header fields and the Contact header from the response in order to release the dialog if needed.

When the S-CSCF receives from the served user a subsequent request other than 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) 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.

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 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 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;

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 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 determined in the previous step;

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

13) 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 1xx or 2xx 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 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 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 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 1xx or 2xx 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.

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.

PROPOSED CHANGE

5.4.4.2.1 Mobile-originating case

When the S-CSCF receives any 1xx response, the S-CSCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present. The term-ioi parameter identifies the sending network of the response message. The term-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS.

When the S-CSCF receives any 1xx or 2xx response, 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 AS.

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

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

PROPOSED CHANGE

5.4.4.2.2 Mobile-terminating case

When the S-CSCF sends any 1xx response, the S-CSCF shall insert an term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi.

When the S-CSCF receives the any 1xx or 2xx response, 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 AS.

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

When the S-CSCF receives any request or response (excluding ACK requests and CANCEL requests and responses) related to a mobile-originated dialog or standalone transaction, the S-CSCF may insert previously saved values into P-

Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message within the S-CSCF home network, including towards AS.

CR-Form-v7

CHANGE REQUEST

⌘	**24.229** CR **429**	⌘**rev**	**-**	⌘	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 **X**

Title: ⌘	BGCF procedure tidyup	
Source: ⌘	Lucent Technologies	
Work item code:⌘	IMS-CCR	***Date:*** ⌘ 02/05/03
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: ⌘	1.	Subclause 5.6.1, 2nd paragraph. Inclusion of the P-Charging-Vector and P-Charging-Functional-Addresses header into ACK and CANCEL is precluded by RFC 3455, and therefore this restriction also needs to be written into this paragraph, where such inclusion is currently allowed. The text is therefore modified accordingly.

Summary of change: ⌘	See above
Consequences if not approved: ⌘	Unclear specification

Clauses affected: ⌘	5.6.1

	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.

5.6 Procedures at the BGCF

5.6.1 General

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

When the BGCF receives any request or response (excluding ACK requests and CANCEL requests and responses) related to a dialog or standalone transaction, the BGCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before forwarding the message.

CR-Form-v7

CHANGE REQUEST

| ⌘ | **24.229** CR **430** | ⌘**rev** | **-** | ⌘ | 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 **X**

Title: ⌘	AS procedure tidyup		
Source: ⌘	Lucent Technologies		
Work item code:⌘	IMS-CCR	***Date:*** ⌘	02/05/03
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: ⌘	1. Subclause 5.7.1.2, 2nd paragraph. Inclusion of the P-Charging-Vector and P-Charging-Functional-Addresses header into ACK and CANCEL is precluded by RFC 3455, and therefore this restriction also needs to be written into this paragraph, where such inclusion is currently allowed. The text is therefore modified accordingly. 2. Subclause 5.7.1.3, 1st paragraph. Inclusion of the P-Access-Network-Info header into ACK and CANCEL is precluded by RFC 3455, and therefore this restriction also needs to be written into this paragraph, where such inclusion is currently assumed. The text is therefore modified accordingly. 3. Subclause 5.7.2, 1st paragraph. The text talks about the following paragraphs being noted. This is not an optimum word to use in a specification, as it could mislead readers to believe the following paragraphs are normative. The word has therefore been changed. 4. Subclause 5.7.3, 1st paragraph. The text talks about the following paragraphs being noted. This is not an optimum word to use in a specification, as it could mislead readers to believe the following paragraphs are normative. The word has therefore been changed. 5. Subclause 5.7.5.2.1, last paragraph. The text currently does not read correctly for the condition, so the word "is" is inserted. 6. Subclause 5.7.5.4. There is a requirement here written in the passive sense which would be clearer written in the active sense.
Summary of change: ⌘	See above
Consequences if not approved: ⌘	Unclear specification
Clauses affected: ⌘	5.7.1.2, 5.7.1.3, 5.7.2, 5.7.3, 5.7.5.2.1, 5.7.5.4

	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.

PROPOSED CHANGE

5.7.1.2　　Extracting charging correlation information

When an AS receives an initial request for a dialog or a request for a standalone transaction, the AS shall store the values received in the P-Charging-Vector header, e.g. icid parameter, and retain the P-Charging-Vector header in the message. The AS shall store the values received in the P-Charging-Function-Addresses header and retain the P-Charging-Function-Addresses header in the message.

When an AS sends any request or response (excluding ACK requests and CANCEL requests and responses) related to a dialog or standalone transaction, the AS may insert previously saved values into the P-Charging-Vector and P-Charging-Function-Addresses headers before sending the message.

PROPOSED CHANGE

5.7.1.3　　Access-Network-Info

The AS may receive in any request or response (excluding ACK requests and CANCEL requests and responses) information about the served user access network. This information is contained in the P-Access-Network-Info header. The AS can use the header to provide an appropriate service to the user.

PROPOSED CHANGE

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

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

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

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

PROPOSED CHANGE

5.7.3　　Application Server (AS) acting as originating UA

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

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

When an AS acting as an originating UA generates an initial request for a dialog or a request for a standalone transaction, the AS shall create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header. The AS may retrieve CCF and/or ECF adresses from HSS on Sh interface.

The AS shall extract charging function addresses from any P-Charging-Function-Addresses header that is received in any 1xx or 2xx responses to the requests.

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

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

PROPOSED CHANGE

5.7.5.2.1 Initial INVITE

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

- remove its own SIP URL from the topmost Route header of the received INVITE request;

- perform the Application Server specific functions. See 3GPP TS 23.218 [5];

- if successful, generate and send a new INVITE request to the S-CSCF to establish a new dialog;

- copy the remaining Route header(s) unchanged from the received INVITE request to the new INVITE request;

- route the new INVITE request based on the topmost Route header.

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

When the AS is acting as an Initiating B2BUA, the AS shall apply the procedures described in subclause 5.7.3 for both requests. The AS shall either set the icid parameter in the P-Charging-Vector header to be the same as received or different. The AS may retrieve CCF and/or ECF adresses from HSS on Sh interface.

PROPOSED CHANGE

5.7.5.4 Call-related requests

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

CR-Form-v7

CHANGE REQUEST

⌘   **24.229** CR **431**   ⌘**rev** **-** ⌘ 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 **X**

Title: ⌘	MRFC procedure tidyup
Source: ⌘	Lucent Technologies
Work item code:⌘	IMS-CCR **Date:** ⌘ 02/05/03
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: ⌘	1. Subclause 5.8.1, 2nd paragraph. Inclusion of the P-Charging-Vector and P-Charging-Functional-Addresses header into ACK and CANCEL is precluded by RFC 3455, and therefore this restriction also needs to be written into this paragraph, where such inclusion is currently allowed. The text is therefore modified accordingly.
Summary of change:⌘	See above
Consequences if not approved: ⌘	Unclear specification

Clauses affected: ⌘	5.8.1

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

Other comments: ⌘	

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

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

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

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

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

5.8.1 General

Although the MRFC is acting as a UA, it is outside the scope of this specification how the MRFC associated addresses are made known to other entities.

When the MRFC sends any request or response (excluding ACK requests and CANCEL requests and responses) related to a dialog or standalone transaction, the MRFC may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before sending the message.

CR-Form-v7

CHANGE REQUEST

| ⌘ | **24.229** CR **434** | ⌘**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 **X**

Title:	⌘	SDP procedure tidyup
Source:	⌘	Lucent Technologies
Work item code: ⌘	IMS-CCR	**Date:** ⌘ 12/05/2003
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: ⌘	1. Subclause 6.2, 1st paragraph. The procedure specified here is only possible for requests. It is not possible to specify a response to a response. Therefore it is proposed to modify the text to make it only applicable to requests (two instances). 2. Subclause 6.2, 2nd paragraph. There is a mandatory modal auxiliary verb in this paragraph that conveys a requirement on the UE, yet the scope of the paragraph is to the P-CSCF. It is proposed that the this is changed to "is". 3. Subclause 6.3, 1st paragraph. The procedure specified here is only possible for requests. It is not possible to specify a response to a response. Therefore it is proposed to modify the text to make it only applicable to requests (two instances).
Summary of change: ⌘	As above
Consequences if not approved: ⌘	As above

Clauses affected: ⌘	6.2, 6.3

	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.

6.2 Procedures at the P-CSCF

When the P-CSCF receives any SIP request ~~or response~~ containing SDP, the P-CSCF shall examine the media parameters in the received SDP. If the P-CSCF finds any media parameters which are not allowed on the network by local policy, the P-CSCF shall return a 488 (Not Acceptable Here) response containing SDP payload. This SDP payload contains either all the media types, codecs and other SDP parameters which are allowed according to the local policy, or, based on configuration by the operator of the P-CSCF, a subset of these allowed parameters. This subset may depend on the content of the received SIP request ~~or response~~. The P-CSCF shall build the SDP payload in the 488 (Not Acceptable Here) response in the same manner as a UAS builds the SDP in a 488 (Not Acceptable Here) response as specifed in RFC 3261 [26]. The P-CSCF shall order the SDP payload with the most preferred codec listed first.

When the P-CSCF receives an initial INVITE request for a terminating session setup or a 183 (Session Progress) response to an INVITE request for an originating session setup, the P-CSCF may modify the SDP according to draft-ietf-mmusic-reservation-flows-01 [54] to indicate to the UE that particular media stream(s) ~~shall be~~ is grouped according to a local policy. The policy is used to determine whether the P-CSCF will request the UE to keep media stream(s) grouped in different PDP contexts and identify the relation between different media streams and PDP contexts (see subclause 9.2.5).

The P-CSCF shall apply and maintain the same policy within the SDP from the initial request or response containing SDP and throughout the complete SIP session. If a media stream is added and grouping apply to the session, the P-CSCF shall modify the SDP according to draft-ietf-mmusic-reservation-flows-01 [54] to indicate to the UE that the added media stream(s) will be grouped into either a new group or into one of the existing groups. The P-CSCF shall not indicate re-grouping of media stream(s) within the SDP.

The P-CSCF shall not apply draft-ietf-mmusic-reservation-flows-01 [54] to the SDP for additional media stream(s), if grouping of media stream(s) was not indicated in the initial INVITE request or 183 (Session Progress) response.

6.3 Procedures at the S-CSCF

When the S-CSCF receives any SIP request ~~or response~~ containing SDP, the S-CSCF shall examine the media parameters in the received SDP. If the S-CSCF finds any media parameters which are not allowed based on either local policy or the subscription, the S-CSCF shall return a 488 (Not Acceptable Here) response containing SDP payload. This SDP payload contains either all the media types, codecs and other SDP parameters which are allowed according to the local policy and users subscription or, based on configuration by the operator of the S-CSCF, a subset of these allowed parameters. This subset may depend on the content of the received SIP request ~~or response~~. The S-CSCF shall build the SDP payload in the 488 (Not Acceptable Here) response in the same manner as a UAS builds the SDP in a 488 (Not Acceptable Here) response as specified in RFC 3261 [26].

CR-Form-v7

CHANGE REQUEST

⌘	**24.229** CR ⁴³⁸	⌘**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 **X** Radio Access Network ☐   Core Network **X**

Title:	⌘	Profile Tables – Further 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 set of problems have been identified in the Tables in Annex A of 24.229. Please note that these problems do only reflect the outcome of a very first check of these tables – more changes will be identified in the future after more detailed review:

1) Table A.119, item 5 indicates that the Authorization header is n/a in the REGISTER request – this is not in-line with e.g. 5.1.1.2 where it is said:

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;

Therefore the authorization header is set to m in Table A.119. |

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

Table A.119: Supported headers within the REGISTER request

Item	Header	Sending			Receiving		
		Ref.	RFC status	Profile status	Ref.	RFC status	Profile status
1	Accept	[26] 20.1	o	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	c1	c1
5	Authorization	[26] 20.7	c2	n/a	[26] 20.7	m	c10
6	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
7	Call-Info	[26] 20.9	o	o	[26] 20.9	o	o
8	Contact	[26] 20.10	o	o	[26] 20.10	m	m
9	Content-Disposition	[26] 20.11	o	o	[26] 20.11	m	m
10	Content-Encoding	[26] 20.12	o	o	[26] 20.12	m	m
11	Content-Language	[26] 20.13	o	o	[26] 20.13	m	m
12	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
13	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
14	Cseq	[26] 20.16	m	m	[26] 20.16	m	m
15	Date	[26] 20.17	c3	c3	[26] 20.17	m	m
16	Expires	[26] 20.19	o	o	[26] 20.19	m	m
17	From	[26] 20.20	m	m	[26] 20.20	m	m
18	Max-Forwards	[26] 20.22	o	o	[26] 20.22	n/a	n/a
19	MIME-Version	[26] 20.24	o	o	[26] 20.24	m	m
20	Organization	[26] 20.25	o	o	[26] 20.25	o	o
20A	Path	[35] 4	c4	c5	[35] 4	m	c6
20B	Privacy	[33] 4.2	c9	n/a	[33] 4.2	c9	n/a
21	Proxy-Authorization	[26] 20.28	c8	c8	[26] 20.28	n/a	n/a
22	Proxy-Require	[26] 20.29	o	o (note)	[26] 20.29	n/a	n/a
23	Require	[26] 20.32	o	o	[26] 20.32	m	m
24	Route	[26] 20.34	o	n/a	[26] 20.34	n/a	n/a
25	Supported	[26] 20.37	o	o	[26] 20.37	m	m
26	Timestamp	[26] 20.38	m	m	[26] 20.38	c7	c7
27	To	[26] 20.39	m	m	[26] 20.39	m	m
28	User-Agent	[26] 20.41	o	o	[26] 20.41	o	o
29	Via	[26] 20.42	m	m	[26] 20.42	m	m

c1:	IF A.4/20 THEN m ELSE n/a - - SIP specific event notification extension.
c2:	IF A.4/8 THEN m ELSE n/a - - authentication between UA and registrar.
c3:	IF A.4/11 THEN o ELSE n/a - - insertion of date in requests and responses.
c4:	IF A.4/24 THEN o ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.
c5:	IF A.4/24 THEN x ELSE n/a - - session initiation protocol extension header field for registering non-adjacent contacts.
c6:	IF (A.3/4) OR A.3/1 THEN m ELSE n/a. - - S-CSCF or UE.
c7:	IF A.4/6 THEN m ELSE n/a - - timestamping of requests.
c8:	IF A.4/8A THEN m ELSE n/a - - authentication between UA and proxy.
c9:	IF A.4/26 THEN o ELSE n/a - - a privacy mechanism for the Session Initiation Protocol (SIP).
c10:	IF A.3/1 THEN m ELSE A4/8 - - UE
NOTE:	No distinction has been made in these tables between first use of a request on a From/To/Call-ID combination, and the usage in a subsequent one. Therefore the use of "o" etc. above has been included from a viewpoint of first usage.

CR-Form-v7

CHANGE REQUEST

| ⌘ | **24.229** CR **439** | ⌘ **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 **X**

| **Title:** | ⌘ | AS's subscription for the registration state event package |

| **Source:** | ⌘ | Nokia |

| **Work item code:** | ⌘ | IMS-CCR | **Date:** ⌘ | 06/05/2003 |

| **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:** | ⌘ | There are no procedures desribing the AS's subscription for the registration state event package |

| **Summary of change:** | ⌘ | Procedure description added |

| **Consequences if not approved:** | ⌘ | Requirements in 23.218 are not fulfilled |

| **Clauses affected:** | ⌘ | 5.7.1.1 |

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

| **Other comments:** | ⌘ | |

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

5.7.1.1 Notification about registration status

The AS may support the REGISTER method in order to discover the registration status of the user. If a REGISTER request arrives containing information about the user's registration status and the AS supports the REGISTER method, the AS shall store the Expires parameter from the request and generate a 200 (OK) response or an appropriate failure response. For the success case, the 200 (OK) response shall contain Expires value equal to the value received in the REGISTER request. The AS shall store the values received in P-Charging-Function-Addresses header. Also, the AS shall store the values of the icid parameter in the P-Charging-Vector header from the REGISTER request.

Upon receipt of a third-party REGISTER request, the AS may subscribe to the reg event package for the public user identity registered at the users registrar (S-CSCF) as described in draft-ietf-sipping-reg-event-00 [43].

On sending a SUBSCRIBE request, the AS shall populate the header fields as follows:

   a) a Request URI set to the resource to which the AS wants to be subscribed to, i.e. to a SIP URI that contains the public user identity of the user that was received in the To header field of the third-party REGISTER request;

   b) a From header field set to the AS's SIP URI;

   c) a To header field, set to a SIP URI that contains the public user identity of the user that was received in the To header field of the third-party REGISTER request; and

   d) an Event header set to the "reg" event package;

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

CR-Form-v7

CHANGE REQUEST

| ⌘ | **24.229** CR **440** | ⌘**rev** | **-** | ⌘ | 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 **X** Radio Access Network ☐   Core Network **X**

Title: ⌘	Temporary Pubilc User Identity in re- and de-REGISTER requests	
Source: ⌘	Nokia	
Work item code: ⌘	IMS-CCR	**Date:** ⌘ 12/05/2003
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: ⌘	24.229 does not state clearly which public user identities should be used for re- and de-registration in case a temporary public user identity was used for initial registration.
Summary of change: ⌘	Temporary public user identity shall be used also for de- and re-registration in order to be in-line with SIP RFC 3261
Consequences if not approved: ⌘	24.229 unclear. Implementations might be non in-line with generic SIP procedures for IMS.

Clauses affected: ⌘	5.1.1.1A

	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.

5.1.1.1A   Parameters contained in the UICC

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

- the private user identity;

- one ore more public user identities; and

- the home network domain name used to address the SIP REGISTER request

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

- generate a private user identity;

- generate a temporary public user identity; and

- generate a home network domain name to address the SIP REGISTER request to.

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

The temporary public user identity is only used in REGISTER requests, i.e. initial registration, re-registration, mobile-initiated deregistration. After a successful registration, the UE will get the associated public user identities, and the UE may use any of them in subsequent non-REGISTER messagesrequests.

The UE shall not reveal to the user the temporary public user identity if the temporary public user identity is barred. The temporary public user identity is not barred if received by the UE in the P-Associated-URI header.