3GPP TSG CN Plenary Meeting #20 **NP-030279**
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 5**

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	397	2	F	Rel-5	Notification about registration state	5.4.0	5.5.0	N1-30	N1-030926
24.229	398		F	Rel-5	Combined CRs: N1-030495, N1-030558 , and N1-030559	5.4.0	5.5.0	N1-30	N1-030646
24.229	402	1	F	Rel-5	Handling of P-Asserted ID in MGCF	5.4.0	5.5.0	N1-30	N1-030848
24.229	404	1	F	Rel-5	S-CSCF initiated release of calls to circiut switched network	5.4.0	5.5.0	N1-30	N1-030873
24.229	405	2	F	Rel-5	Supported Integrity algorithms	5.4.0	5.5.0	N1-30	N1-030927
24.229	407	1	F	Rel-5	RFC 3524, Single Reservation Flows	5.4.0	5.5.0	N1-30	N1-030851
24.229	410	1	F	Rel-5	Clarification of the S-CSCF's handling of the P-access-network-info header	5.4.0	5.5.0	N1-30	N1-030868
24.229	411	2	F	Rel-5	Port numbers in the RR header entries	5.4.0	5.5.0	N1-30	N1-030941
24.229	412	2	F	Rel-5	Registration abnormal cases	5.4.0	5.5.0	N1-30	N1-030928

3GPP TSG-CN1 Meeting #30 *Tdoc N1-030926*
San Diego, California, USA, 19 – 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **CR 397** ⌘ **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:	⌘	Notification about registration state
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:	⌘	The S-CSCF should generate a NOTIFY request on all dialogs which have been established due to subscription to the reg event package, when the contact information of the public user identity changes, inspite of the state staying the same.
Summary of change:	⌘	Relevant text added.
Consequences if not approved:	⌘	Incomplete specification

Clauses affected:	⌘	5.4.2.1.2

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.

5.4.2.1.2 Notification about registration state

~~If the registration state of one or more public user identities changes, the S-CSCF shall generate a~~For each NOTIFY request on all 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; and

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; and

   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", "expired", "unregistered" or "probation" according draft-ietf-sipping-reg-event-00 [43]; or

      II) has been registered then:

         - set the state attribute within the <registration> element to "active";

         - set the state attribute within the <contact> element to "active"; and

         - set the event attribute within the <contact> element to "registered"; or

      III) has been automatically registered:

         - set the state attribute within the <registration> element to "active";

         - set the state attribute within the <contact> element to "active"; and

         - set the event attribute within the <contact> element to "created".

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

EXAMPLE: If sip:user1_public1@home1.net is registered, the public user identity sip:user1_public2@home1.net can automatically be registered. Therefore the entries in the body of the NOTIFY request look like:

```
<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
             version="0" state="full">
  <registration aor="sip:user1_public1@home1.net" id="as9"
                state="active">
    <contact id="76" state="active" event="registered"
           >sip:[5555::aaa:bbb:ccc:ddd]</contact>
  </registration>
  <registration aor="sip:user1_public2@home1.net" id="as10"
                state="active">
    <contact id="86" state="active" event="created"
           >sip:[5555::aaa:bbb:ccc:ddd]</contact>
  </registration>
</reginfo>
```

3GPP TSG-CN1 Meeting #30 ***Tdoc N1-030646***
San Diego, California, USA, 19 - 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **398** ⌘ **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 ☒

Title:	⌘	Combined CRs: N1-030495 (Lucent), N1-030558 (Nokia), and N1-030559(Nokia)
Source:	⌘	Nokia, 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:	⌘	The CRs N1-030495, N1-030558, and N1-030559 were addressing different issues in the subclause 5.2.5.1 of the document TS 24.229. To facilitate the inclusion of the respective CRs into the document TS 24.229, this CR combines all three CRs into a single CR.
Summary of change:	⌘	The text in the CRs N1-030495, N1-030558, and N1-030559 were combined together.
Consequences if not approved:	⌘	The editor will have to incorporate each individual CR into the 24.229 document.

Clauses affected:	⌘	5.1.1.6 and 5.2.5.1

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

Other comments:	⌘	Revised as requested by Nokia.

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 other remaining public user identities registered, the UE shall update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities.

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 there are other remaining public user identities registered, the UE shall update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities.~~

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.

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. Due to that, the P-CSCF shall:

- if there are other remaining public user identities registered, the P-CSCF shall update the SIP level lifetime of the security association to the longest registration expiration time of the remaining public user identities; or

- If When all of the public user identities of a user are deregistered, the P-CSCF shall,

  - remove the security associations towards that user after the server transaction (as defined in RFC 3261 [26]) pertaining to this deregistration terminates.; and

  - 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: Deleting a security association is an internal procedure of the P-CSCF and does not involve any SIP procedures.

NOTE 21: 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 32: When the P-CSCF has sent the 200 (OK) 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 contaning the deregistration event) will not reach the UE.

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **402** ⌘ **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:	⌘	Handling of P-Asserted-ID in MGCF
Source:	⌘	SIEMENS
Work item code:	⌘	IMS-CCR
Date:	⌘	23/04/2003
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:	⌘	In 24.229 it is stated that in case of a IMS->PSTN call the MGCF shall set up the p-asserted-id header in 183 Session Progress. But when sending the 183 Response the MGCF has no knowledge of the identiy of the connected party.
Summary of change:	⌘	P-Asserted-ID in case of IMS-PSTN call must be provided by the MGCF only after MGCF has knowledge of identity of connected party. This is after having received the first backward message from PSTN.
Consequences if not approved:	⌘	COLP feature does not work for IMS->PSTN call

Clauses affected:	⌘	5.5.3.1.2, 5.5.3.2.2

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.

5.5 Procedures at the MGCF

5.5.1 General

The MGCF, 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. Therefore table A.4/1 and dependencies on that major capability shall not apply.

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

When the MGCF sends any request or response related to a dialog or standalone transaction, the MGCF may insert previously saved values into P-Charging-Vector and P-Charging-Function-Addresses headers before sending the message.

5.5.2 Subscription and notification

Void.

5.5.3 Call initiation

5.5.3.1 Initial INVITE

5.5.3.1.1 Calls originated from circuit-switched networks

When the MGCF receives an indication of an incoming call from a circuit-switched network, the MGCF shall:

- generate and send an INVITE request to I-CSCF:
  - set the Request-URI to the "tel" format using an E.164 address;
  - set the Supported header to "100rel" (see RFC 3312 [30]);
  - include an P-Asserted-Identity header;
  - create a new, globally unique value for the icid parameter and insert it into the P-Charging-Vector header; and
  - insert an orig-ioi parameter into the P-Charging-Vector header. The orig-ioi parameter shall be set to a value that identifies the sending network in which the MGCF resides and the term-ioi parameter shall not be included.

5.5.3.1.2 Calls terminating in circuit-switched networks

When the MGCF receives an initial INVITE request with Supported header indicating "100rel", the MGCF shall:

- send 100 (Trying) response;
- after a matching codec is found at the MGW, send 183 "Session Progress" response:
  - set the Require header to the value of "100rel";
  - ~~include an P-Asserted-Identity header;~~
  - store the values received in the P-Charging-Function-Addresses header;
  - store the value of the icid parameter received in the P-Charging-Vector header; and
  - insert a term-ioi parameter into the P-Charging-Vector header. The term-ioi parameter shall be set to a value that identifies the network in which the MGCF resides.

When the MGCF does not find an available matching codec at the MGW for the received initial INVITE request, the MGCF shall:

- send 503 (Service Unavailable) response if the type of codec was acceptable but none were available; or
- send 488 (Not Acceptable Here) response if the type of codec was not supported, and may include SDP in the message body to indicate the codecs supported by the MGCF/MGW.

5.5.3.2 Subsequent requests

5.5.3.2.1 Calls originating in circuit-switched networks

When the MGCF receives 183 response to an INVITE request, the MGCF shall:

- store the values received in the P-Charging-Function-Addresses header.

When the MGCF receives 200 (OK) response to a PRACK request and notification that bearer setup is complete, the MGCF shall:

- send an UPDATE request.

5.5.3.2.2 Calls terminating in circuit-switched networks

When the MGCF receives an indication of a ringing for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 180 Ringing to the UE.

When the MGCF receives an indication of answer for the called party of outgoing call to a circuit-switched network, the MGCF shall:

- send 200 OK to the UE, including an P-Asserted-Identity header.

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **404** ⌘ **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:	⌘	S-CSCF initiated release of calls to circuit switched network
Source:	⌘	Siemens
Work item code:	⌘	IMS-CCR
Date:	⌘	23/04/2003
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:	⌘	Missing description in 24.229 of the handling of IMS initiated call release in the MGCF when IMS interworks with circuit switched networks.
Summary of change:	⌘	Insert a note saying that releasing a call towards the circuit switched network additionally requires singnaling procedures that are outside the scope of the specification.
Consequences if not approved:	⌘	Incomplete specification

Clauses affected:	⌘	5.5.4.2			
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.

5.5.4 Call release

5.5.4.1 Call release initiated by a circuit-switched network

When the MGCF receives an indication of call release from a circuit-switched network, the MGCF shall:

- send a BYE request to the UE.

5.5.4.2 ~~S-CSCF~~ IM CN subsystem initiated call release

NOTE: The release of a call towards the circuit-switched network additionally requires signaling procedures other than SIP in the MGCF that are outside the scope of this document.

5.5.4.3 MGW-initiated call release

When the MGCF receives an indication from the MGW that the bearer was lost, the MGCF shall:

- send a BYE request towards the UE; and
- may include Error-Info header witha pointer to additional information indicating that bearer was lost.

5.5.5 Call-related requests

5.5.5.1 ReINVITE

5.5.5.1.1 Calls originating from circuit-switched networks

Void.

5.5.5.1.2 Calls terminating in circuit-switched networks

When the MGCF receives a reINVITE request for hold/resume operation, the MGCF shall:

- send 100 (Trying) response;
- after performing interaction with MGW to hold/resume the media flow, send 200 (OK) response.

5.5.6 Further initial requests

When the MGCF responds to an OPTIONS request with a 200 (OK) response, the MGCF may include a message body with an indication of the DTMF capabilities and supported codecs of the MGCF/MGW.

NOTE: The detailed interface for requesting MGCF/MGW capabilities is not specified in this version of the document. Other solutions may be used in the interim.

3GPP TSG-CN1 Meeting #30 ***Tdoc N1-030927***
San Diego, California, USA, 19 – 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **405** ⌘**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:	⌘	Supported Integrity algorithms
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	20/05/2003
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 specification does not elaborate on the supported integrity algoritms
Summary of change:	⌘	The UE shall support MD5 and SHA-1 IPsec integrity algoritms. The UE has to announce its support in the Security-Client header. The P-CSCF shall support MD5 and SHA-1 and announces its support in the Security-Server header.
Consequences if not approved:	⌘	Not compliant with the stage 2 specifications

Clauses affected:	⌘	2, 5.1.1.2, 5.2.2

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

Other comments:	⌘	

First proposed change

2 References

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

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

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

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

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

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

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

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

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

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

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

[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".

[20B] RFC 2403 (November 1998) "The Use of HMAC-MD5-96 within ESP and AH".

[20C] RFC 2404 (November 1998) "The Use of HMAC-SHA-1-96 within ESP and AH".

[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)"

Next proposed change

5.1.1.2 Initial registration

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

A REGISTER request may be integrity protected using IK, see 3GPP TS 33.203 [19], derived as a result of an earlier registration.

The public user identity to be registered can be extracted either from the ISIM application, if present, on the UICC or derived from the USIM, according to the procedures described in subclause 5.1.1.1A. A public user identity may be input by the end user.

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

a) the 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 registered;

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

d) the Contact header set to include SIP URI(s) containing the IP address of the UE in the hostport parameter or FQDN. If the protected port value that is bound to the security association is known by the UE, that shall be also included in the hostport parameter;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

e) the Expires header, or the expires parameter within the Contact header, set to the value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 2: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

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

g) the Security-Client header field set to specify the security mechanism the UE supports, the IPSec layer algorithms the UE supports and the parameters needed for the security association setup. ~~For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]~~ The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 [20B] and HMAC-SHA-1-96 [20C] IPsec layer algorithms and shall announce support for them according to the procedures defined in RFC 3329 [48];

h) the Supported header containing the option tag "path"; and

i) if a security association exists, 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 store the expiration time of the registration for the public user identities found in the To header value. The UE shall also store the list of URIs contained in the P-Associated-URI header value. This list contains the URIs that are associated to the registered public user identity. The list contains also the identity under registration, unless this identity is barred. In order to build a proper preloaded Route header value for new dialogs, the UE shall also store the list of Service Route headers contained in the Service-Route header.

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

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

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

Next 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. If there is such header, then 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. The P-CSCF shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The P-CSCF shall support the HMAC-MD5-96 [20B] and HMAC-SHA-1-96 [20C] IPsec layer algorithms. 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. 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 requestwas 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.

3GPP TSG-CN1 Meeting #30 ***Tdoc N1-030851***
San Diego, California, USA, 19 – 23 May 2003

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **407** ⌘ **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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	RFC 3524, Single Reservation Flows
Source:	⌘	Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	11/05/2003
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:	⌘	RFC 3524, Single Reservation Flows is available. Old internet draft is obsolete RFC 3515, SIP REFER method is available. Old internet draft is obsolete. Some other internet drafts have got new revisions
Summary of change:	⌘	RFC 3524 replaces draft-ietf-mmusic-reservation-flows-01 throughout the spec RFC 3515 replaces draft-ietf-sip-refer-01 Miscelaneous updates of new versions of Internet Draft
Consequences if not approved:	⌘	References refer to a non available document

Clauses affected:	⌘	2, 6.1, 6.2, 9.2.5.1A

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

⌘

Other comments: ⌘

First proposed change

2 References

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

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

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

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

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

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

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

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

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

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

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

[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".~~RFC 3515 (April 2003): "The Session Initiation Protocol (SIP) 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~~ 04 (~~August 2002~~May 2003): "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~~ 12 (~~May 2002~~March 2003): "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~~ 28 (~~June~~ November 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~~ 01 (~~April~~ November 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".~~RFC 3524 (April 2003): "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)"

Next proposed change

---

6 Application usage of SDP

6.1 Procedures at the UE

Usage of SDP by the UE:

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

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

   a=des: qos mandatory local sendrecv

   a=curr: qos local none

3. Providing that the INVITE request received by the UE contains an SDP offer including one or more "m=" media descriptions, the first 183 (Session Progress) provisional response that the UE sends, shall contain the answer for the SDP received in the INVITE. The said SDP answer shall reflect the called user's terminal capabilities and user preferences.

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

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

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

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

8. The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to ~~draft-ietf-mmusic-reservation-flows-01~~RFC 3524 [54] and perform the action outlined in subclause 9.2.5.

9. If a PDP context is rejected or modified, the UE shall, if the SDP is affected, update the remote SIP entity according to RFC 3261 [26] and RFC 3311 [29].

10. If the UE builds SDP for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE: The UE may be attempting a session establishment through multiple networks with different policies and potentially may need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE 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~~RFC 3524 [54] to indicate to the UE that particular media stream(s) shall be 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~~RFC 3524 [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~~RFC 3524 [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.

Next proposed change

9.2.5 PDP contexts for media

9.2.5.1 General requirements

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

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

9.2.5.1A Activation or modification of PDP contexts for media

If the UE receives indication within the SDP according to ~~draft-ietf-mmusic-reservation-flows-01~~RFC 3524 [54] that media stream(s) belong to group(s), the media stream(s) shall be set up on separate PDP contexts according to the indication of grouping. The UE may freely group media streams to PDP context(s) in case no indication of grouping is received from the P-CSCF.

The UE can receive a media authorization token in the P-Media-Authorization header from the P-CSCF according to RFC 3313 [31]. The UE shall, if a media authorization token is received in the P-Media-Authorization header when a SIP session is initiated, establish separate PDP context(s) for the media. If a media authorization token is received in subsequent messages for the same SIP session, the UE shall:

- use the existing PDP context(s) for media;
- modify the existing PDP context(s) for media; or
- establish additional PDP context(s) for media.

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

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

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

If the UE receives several media authorization tokens from the P-CSCF within the same SIP request or response, the first instance of the media authorization token shall be sent to the GGSN, and subsequent instances are discarded by the UE.

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

9.2.5.2 Special requirements applying to forked responses

Since the UE does not know that forking has occurred until a second, provisional response arrives, the UE sets up the PDP context(s) as required by the initial response received. If a subsequent provisional response is received, different alternative actions may be performed depending on the requirements in the SDP answer:

1) **the bearer requirements of the subsequent SDP can be accommodated by the existing PDP context(s).** The UE performs no activation or modification of PDP contexts.

2) **the subsequent SDP introduces different QoS requirements or additional IP flows.** The UE modifies the existing PDP context(s), if necessary, according to subclause 9.2.5.1A.

3) **the subsequent SDP introduces one or more additional IP flows.** The UE establishes additional PDP context(s) according to subclause 9.2.5.1A.

NOTE 1: When several forked responses are received, the resources requested by the UE is are the "logical OR" of the resources indicated in the multiple responses to avoid allocation of unnecessary resources. The UE does not request more resources than proposed in the original INVITE request.

NOTE 2: When service-based local policy is applied, the UE receives the same authorization token for all forked requests/responses related to the same SIP session.

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall release all the unneeded radio/bearer resources. Therefore, upon the reception of a first final 200 (OK) response for the INVITE request (in addition to the procedures defined in RFC 3261 [26] subclause 13.2.2.4), the UE shall:

1) in case PDP context(s) were established or modified as a consequence of the INVITE request and forked provisional responses that are not related to the accepted 200 (OK) response, delete the PDP context(s) or modify the delete the PDP context(s) back to their original state.

9.2.5.3 Unsucessful situations

One of the Go interface related error codes can be received by the UE in the ACTIVATE SECONDARY PDP CONTEXT REJECT message or the MODIFY PDP CONTEXT REJECT message. If the UE receives a Go interface related error code, the UE shall either terminate the session or retransmit the message up to three times. The Go interface related error codes are further specified in 3GPP TS 29.207 [12].

3GPP TSG-CN1 Meeting #30 *Tdoc N1-030868*
San Diego, California, USA, 19 – 23 May 2003 (Revision of N1-030708)

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **410** ⌘ **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:	⌘	Clarification of the S-CSCF's handling of the P-access-network-info header
Source:	⌘	Vodafone
Work item code:	⌘	IMS-CCR
Date:	⌘	09/05/2003
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:	⌘	Currently, section 5.4.3.2 creates confusion as to whether or not the p-access-network-info header should be removed from a SIP message if the 'destination network' it is being routed towards is the same network as the home network. This could lead to the p-access-network-info header being transferred all the way to a UE. This is not allowed.
Summary of change:	⌘	The phrase 'destination network' is removed and it is clarified that the S-CSCF, when routing the SIP message to the destination user, shall always remove the p-access-network-info header.
Consequences if not approved:	⌘	There will be a risk of an end-user finding out the cell-id of another user.

Clauses affected:	⌘	5.4.3.2

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

Other comments: ⌘

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

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

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

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

********** FIRST MODIFIED SECTION **********

4.4 Trust domain

RFC 3325 [34] provides for the existence and trust of an asserted identity within a trust domain. For the IM CN subsystem, this trust domain consists of the P-CSCF, the I-CSCF, the S-CSCF, the BGCF. the MGCF, the MRFC, and all ASs that are not provided by third-party service providers. ASs provided by third-party service providers are outside the trust domain.

For the purpose of the P-Access-Network-Info header, a trust domain also applies. This trust domain is identical to that of the P-Asserted-Identity. For the P-Access-Network-Info header, subclause 5.4 also identifies additional cases for the removal of the header.

NOTE: In addition to the procedures specified in clause 5, procedures of RFC 3325 [34] in relation to transmission of P-Asserted-Identity headers and their contents outside the trust domain also apply.

********** SECOND MODIFIED SECTION **********

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, 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) remove the P-Access-Network-Info header prior to forwarding the message based on the destination user (Request-URI) ~~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 response to the initial request for a dialog, it shall save the necessary Record-Route header fields and the Contact header from the response in order to release the dialog if needed.

When the S-CSCF receives from the served user a 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 routed towards the destination user (Request-URI)~~forwarded to the destination network~~ or is routed 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 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 routed towards the destination user (Request-URI)~~forwarded to the destination network~~ or is routed 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.

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

Tdoc ⌘N1-030~~716~~941~~849~~

CR-Form-v7

CHANGE REQUEST

⌘	24.229	CR	411	⌘rev	2 ~~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:	⌘	Port numbers in the RR header entries
Source:	⌘	Nokia, Lucent
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:	⌘	Currently in the TS it is said that the P-CSCF inserts the port number of the UE into the RR header entries. While this is right in one direction, it has to be rewritten in responses in order to allow allow subsequent requests from that direction also.
Summary of change:	⌘	Port number rewriting has been applied to responses, comp parameter addition has been specified.
Consequences if not approved:	⌘	Not working procedures.

Clauses affected:	⌘	5.2.6.3, 5.2.6.4			
Other specs affected:	⌘	**Y**	**N**	Other core specifications	⌘
				Test specifications	
				O&M Specifications	
Other comments:	⌘				

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

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

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

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

5.2.6.3 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 address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF in accordance with the procedures of RFC3261 [26], and either:

   a) the P-CSCF FQDN that resolves to the IP address, or

   b) the P-CSCF IP address;

3) add its own SIP URL 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 where it awaits subsequent requests from the called party, 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~~;

4~~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

5~~4~~) 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 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) rewrite the port number of its own Record Route entry to its own protected port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC3486 [55]; and~~.~~

5) save the Contact header received in the response in order to release the dialog 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 address to the Via header. The P-CSCF Via header entry is built in a format that contains the port number of the P-CSCF where it awaits the responses to come, and either:

   a) the P-CSCF FQDN that resolves to the IP address, or

   b) the P-CSCF IP address;

4~~3~~) add its own SIP URL 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 P-CSCF where it awaits subsequent requests from the called party, and either:

   a) the P-CSCF FQDN that resolves to the IP address; or

   b) the P-CSCF IP address;

~~add its own SIP URL 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-CSCF~~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 list of Record-Route headers from the received response;

2) rewrite the port number of its own Record Route entry to its own protected port number negotiated with the calling UE, and append the comp parameter in accordance with the procedures of RFC3486 [55]; and

3~~2~~) save the Contact header received in the response in order to release the dialog 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 from the topmost Route header;

~~2) save the Record-Route header list;~~

2~~3~~) convert the list of Record-Route header values into a list of Route header values and save this list of Route headers;

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

4~~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 comp parameter in accordance with the procedures of RFC3486 [55], and 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;

5~~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 comp parameter in accordance with the procedures of RFC3486 [55], and 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~~7~~) store the values received in the P-Charging-Function-Addresses header;

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

8~~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~~ Record Route header values with those received in the request; rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter.~~;~~

If the verification is successful, the P-CSCF shall rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;

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

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

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

1) 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 from the topmost Route header value;

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

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

4) add its own address to the top of the received list of Via header and save the list. The P-CSCF Via header entry is built in a format that contains the comp parameter in accordance with the procedures of RFC3486 [55], and the port number of the security association established from the UE to the P-CSCF and either:

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

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

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

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

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

   a) discard the response; or

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

2) rewrite the port number of its own Record-Route entry to the port number where it awaits subsequent requests from the calling party and remove the comp parameter;

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 comp parameter in accordance with the procedures of RFC3486 [55], and 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 comp parameter in accordance with the procedures of RFC3486 [55], and 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].

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

Tdoc ⌘N1-030928

CR-Form-v7

CHANGE REQUEST

⌘ **24.229** **CR** **412** ⌘ **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:	⌘	Registration abnormal cases
Source:	⌘	Nokia
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:	⌘	~~Some overlapping text is present in the abnormal cases for the user's registration section. In addition to that, some weird conditions, which have no base are present there.~~The S-CSCF has no means to determine whether a response to the challenge will be received or not. This is handled by the SIP retransmission timers. Another change is needed because one of the error cases, when the MAC parameter derived from AUTN by the UE is invalid, is wrongly specified.
Summary of change:	⌘	~~The overlapping text and the text posing some weird conditions to the S-CSCF has been removed.~~The text when the S-CSCF determines that there won't be response to the challenge is deleted. The error case is clarified.
Consequences if not approved:	⌘	Total confusion on how to handle the abnormal cases.

Clauses affected:	⌘	5.4.1.2.3, 5.1.1.5.3

	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.

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 401 (Unauthorized) 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 which was supposed to carry the response to the challenge ~~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:~~ contains no RES and no AUTS parameters~~,~~ indicat~~es~~ing that the MAC parameter was invalid in the challenge~~. T~~, the S-CSCF shall either:

- respond with a 401 (Unauthorised) containing a new challenge ~~including a valid MAC parameterthe relevant 4xx response (e.g. 401 (Unauthorized)~~ to initiate a further authentication attempt, or

- respond with a 403 (Forbidden) 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 indicating this), 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 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.

5.1.1.5.3 Abnormal cases

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

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

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

A UE shall only respond to two consecutive invalid challenges. The UE may attempt to register with the network again after an implementation specific time. The REGISTER request shall be protected with the existing keys (CK and IK) if available, see 3GPP TS 33.203 [19].