Source:	**TSG CN WG1**
Title:	**CRs to Rel-5 WI IMS-CCR for TS 24.229 (with mirror CRs)and TS 24.228**
Agenda item:	**8.1**
Document for:	**APPROVAL**

This document contains **14 CRs on Rel-5 Work Item "IMS-CCR"**, that have been agreed by TSG CN WG1 CN#36 meeting and forwarded to TSG CN Plenary meeting #26 for approval.

TDoc #	Tdoc Title	Spec	CR #	Rev	CAT	C_Version	WI	Rel
N1-041955	Term IOI in responses	24.229	722	1	F	5.10.0	IMS-CCR	Rel-5
N1-041956	Term IOI in responses	24.229	723	1	A	6.4.0	IMS-CCR	Rel-6
N1-041957	Request handling in S-CSCF originating case	24.229	724	1	F	5.10.0	IMS-CCR	Rel-5
N1-041958	Request handling in S-CSCF originating case	24.229	725	1	A	6.4.0	IMS-CCR	Rel-6
N1-041959	Request handling in S-CSCF - terminating case	24.229	726	1	F	5.10.0	IMS-CCR	Rel-5
N1-041960	Request handling in S-CSCF - terminating case	24.229	727	1	A	6.4.0	IMS-CCR	Rel-6
N1-041961	Population of Via header when using REGISTER method	24.229	737	1	F	5.10.0	IMS-CCR	Rel-5
N1-041962	Population of Via header when using REGISTER method	24.229	738	1	A	6.4.0	IMS-CCR	Rel-6
N1-041965	Interaction between S-CSCF and HSS in Network initiated deregistration procedure	24.229	764	1	F	5.10.0	IMS-CCR	Rel-5
N1-041966	Interaction between S-CSCF and HSS in Network initiated deregistration procedure	24.229	765	1	A	6.4.0	IMS-CCR	Rel-6
N1-041967	Interaction between S-CSCF and HSS in Network initiated deregistration procedure	24.228	136		F	5.10.0	IMS-CCR	Rel-5
N1-042091	Network-initiated deregistration for the old contact information of a roaming UE registered in a new network	24.229	754	1	F	5.10.0	IMS-CCR	Rel-5
N1-042102	Downloading of user profile	24.229	767	1	F	5.10.0	IMS-CCR	Rel-5
N1-042103	Downloading of user profile	24.229	768	1	A	6.4.0	IMS-CCR	Rel-6

CR-Form-v7.1

CHANGE REQUEST

⌘   **24.229** CR **722**   ⌘**rev** **1** ⌘ Current version: **5.10.0** ⌘

*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: ⌘	Term IOI in responses
Source: ⌘	Siemens
Work item code:⌘	IMS-CCR **Date:** ⌘ 17/11/2004

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:
Ph2   (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)
Rel-7   (Release 7)

Reason for change: ⌘	No term-ioi parameter is sent in responses from the terminating network to the originating network in case of requests for standalone transactions
Summary of change:⌘	In case of a response to a request for a standalone transaction include the term-ioi parameter in the p-charging-vector header of a 200 OK
Consequences if not approved: ⌘	Incorrect charging records for standalone requests

Clauses affected: ⌘	5.4.3.2, 5.4.3.3

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

Other comments: ⌘	

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

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

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

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

*** 1ˢᵗ change ***

5.4.3 General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF

5.4.3.1 Determination of mobile-originated or mobile-terminated case

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

- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the request makes use of the information for mobile-originating calls, which was added to the Service-Route header entry of the S-CSCF during registration (see subclause 5.4.1.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter; or,

- perform the procedures for the mobile-terminating case as described in subclause 5.4.3.3 if this information is not used by the request.

5.4.3.2 Requests initiated by the served user

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

1) determine whether the request contains a barred public user identity in the P-Asserted-Identity header field of the request or not. In case the said header field 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;

NOTE 1: If the P-Asserted-Identity header field contains a barred public user identity, then the message has been received, either directly or indirectly, from a non-compliant entity which should have had generated the content with a non-barred public user identity.

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

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

4) check whether the initial request matches the initial filter criteria based on a public user identity in the P-Asserted-Identity header, and if it does, forward this request to that AS, 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 AS 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 AS(s) before processing the outgoing Request-URI. In case of contacting one or more AS(s) the S-CSCF shall:

   a) insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4; 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 URI contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;

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

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

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

12) in case of an initial request for a dialog the S-CSCF shall create a Record-Route header containing its own SIP URI;

13) if the destination user (Request-URI) lies outside of the trust domain of the S-CSCF, remove the P-Access-Network-Info header, prior to forwarding the message;

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

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

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

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

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

NOTE 3: 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 any response to the above request containing a term-ioi parameter, the S-CSCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present. The term-ioi parameter identifies the sending network of the response message. The term-ioi parameter and the orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS.

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response in order to be able to release the session if needed.

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

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

2) create a Record-Route header containing its own SIP URI;

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

4) in case the request is routed towards the destination user (Request-URI)or is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header; and

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

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed.

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

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

2) in case the request is routed towards the destination user (Request-URI)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.

5.4.3.3 Requests terminated at the served user

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

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

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

3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request.

   - If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request.

   - If not present, it indicates that the request is visiting the S-CSCF for the first time, and in this case the S-CSCF shall save the Request-URI from the request;

4) check whether the initial request matches the next unexecuted initial filter criteria in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

NOTE 1: Depending on the result of the previous process, the S-CSCF may contact one or more AS(s) before processing the outgoing Request-URI.

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

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

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

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

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

   b) forward the request based on the Request-URI and skip the following steps;

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

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

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

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

c) build a Request-URI with the contents of the saved Contact URI determined in the previous step; and

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

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

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

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].

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

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

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

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

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

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

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), it shall:

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

2) insert an term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi;

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

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

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

When the S-CSCF receives the 200 (OK) response for a standalone transaction request, the S-CSCF shall:

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

2) insert a term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi.

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

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

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

3) create a Record-Route header containing its own SIP URI; and

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

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog (whether the user is registered or not), the S-CSCF shall:

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

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

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

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

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

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

***next change ***

5.4.4.2 Subsequent requests

5.4.4.2.1 Mobile-originating case

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

When the S-CSCF receives any 1xx or 2xx response, the S-CSCF shall insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

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

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

5.4.4.2.2 Mobile-terminating case

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

When the S-CSCF receives the any 1xx or 2xx response, the S-CSCF shall insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

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

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

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **24.229** CR **723** | ⌘**rev** | **1** | ⌘ | Current version: | **6.4.0** | ⌘ |

*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: ⌘	Term-IOI in response	
Source: ⌘	Siemens	
Work item code:⌘	IMS-CCR	***Date:*** ⌘ 17/11/2004
Category: ⌘ **A**		***Release:*** ⌘ Rel-6

Use <u>one</u> 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 <u>one</u> of the following releases:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change: ⌘	No term-ioi parameter is sent in responses from the terminating network to the originating network in case of requests for standalone transactions In case of INVITE for a dialog without using preconditions (e.g. for a session for MSRP) no term-ioi parameter is sent, as no 1xx responses are sent back.
Summary of change:⌘	In case of a response to a request for a standalone transaction include the term-ioi parameter in the p-charging-vector header of a 200 OK. In case of INVITE for a dialog the term ioi is sent back in 200 ok, too.
Consequences if not approved: ⌘	Incorrect charging records for standalone requests and for session setup for dialogs withou precondtions.

Clauses affected: ⌘	5.4.3, 5.4.4

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

Other comments: ⌘	

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

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

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

*** 1st change ***

5.4.3 General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF

5.4.3.1 Determination of mobile-originated or mobile-terminated case

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

- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the request makes use of the information for mobile-originating calls, which was added to the Service-Route header entry of the S-CSCF during registration (see subclause 5.4.1.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter; or,

- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the topmost Route header of the request contains the "orig" parameter. The S-CSCF shall remove the "orig" parameter from the topmost Route header; or,

- perform the procedures for the mobile-terminating case as described in subclause 5.4.3.3 if this information is not used by the request.

5.4.3.2 Requests initiated by the served user

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

Editor's Note: It needs to be stated, that the S-CSCF will only perform the following steps if the request was received from a trusted entity, e.g. an entity within the trust domain.

1) determine whether the request contains a barred public user identity in the P-Asserted-Identity header field of the request or not. In case the said header field 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;

NOTE 1: If the P-Asserted-Identity header field contains a barred public user identity, then the message has been received, either directly or indirectly, from a non-compliant entity which should have had generated the content with a non-barred public user identity.

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

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

4) check whether the initial request matches the initial filter criteria based on a public user identity in the P-Asserted-Identity header, and if it does, forward this request to that AS, 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 AS 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 AS(s) before processing the outgoing Request-URI. In case of contacting one or more AS(s) the S-CSCF shall:

   a) insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4; 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 URI contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;

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

10) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header if present, otherwise based on the Request-URI. If the destination address is of an IP address type other than the IP address type used in the IM CN subsystem , then the S-CSCF shall forward the request to the IMS-ALG if the IM CN subsytem supports interworking to networks with different IP address type;

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 originated from a served user, either:

- if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or

- if the request is routed elsewhere, create a Record-Route header containing its own SIP URI;

NOTE 2: For requests originated from a PSI the S-CSCF can decide whether to record-route or not.

Editor's Note: It needs to be clarified how the S-CSCF decides whether to put its address into the Record-Route header in the case of handling a request that originates from a PSI. It might be part of the operators policy.

13) based on local policy rules and the destination user (Request-URI), remove the P-Access-Network-Info header prior to forwarding the message;

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

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

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

1) apply any privacy required by RFC 3325 [34] to the P-Asserted-Identity header; and

2) apply the same privacy mechanism to the P-Access-Network-Info header, if present.

NOTE 3: The P-Asserted-Identity header would normally only be expected in 1xx or 2xx responses.

NOTE 4: The optional procedures above are 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 any response to the above request containing a term-ioi parameter, the S-CSCF shall store the value of the received term-ioi parameter received in the P-Charging-Vector header, if present. The term-ioi parameter identifies the sending network of the response message. The term-ioi parameter and the orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS.

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response in order to be able to release the session if needed.

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

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

2) create a Record-Route header containing its own SIP URI;

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

4) in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header;

5) in case the request is routed towards the destination user (Request-URI) based on local policy rules and the destination user (Request-URI), remove the P-Access-Network-Info header; and

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

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed.

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

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

2) in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header; and

3) in case the request is routed towards the destination user (Request-URI) based on local policy rules and the destination user (Request-URI), remove the P-access-network-info header; and

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

5.4.3.3 Requests terminated at the served user

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

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

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

3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request.

   - If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request.

   - If not present, it indicates that the request is visiting the S-CSCF for the first time, and in this case the S-CSCF shall save the Request-URI from the request;

4) check whether the initial request matches the next unexecuted initial filter criteria in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

NOTE 1: Depending on the result of the previous process, the S-CSCF may contact one or more AS(s) before processing the outgoing Request-URI.

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

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

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

8) if necessary perform the caller preferences to callee capabilities matching according to draft-ietf-sip-caller-preferences [62];

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

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

   b) forward the request based on the Request-URI and skip the following steps;

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

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

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

   b) determine, from the destination public user identity, the saved Contact URI where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2. If there is more than one contact address saved for the destination public user identity, the S-CSCF shall:

      - if the fork directive in the Request Disposition header was set to "no-fork", forward the request to the contact with the highest qvalue parameter. In case no qvalue parameters were provided, the S-CSCF shall decide locally how to forward the request; otherwise

      - fork the request or perform sequential search based on the relative preference indicated by the qvalue parameter of the Contact header in the original REGISTER request, as described in RFC3261 [26]. In case no qvalue parameters were provided, then the S-CSCF shall forward the request as directed by the Request Disposition header as described in draft-ietf-sip-callerprefs-10 [56B]. If the Request-Disposition header is not present, the S-CSCF shall decide locally whether to fork or perform sequential search among the contact addresses;

   c) build a Request-URI with the contents of the saved Contact URI determined in the previous step; and

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

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

12) optionally, apply any privacy required by RFC 3325 [34] to the P-Asserted-Identity header and apply the same privacy mechanism to the P-Access-Network-Info header;

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].

13) in case of an initial request for a dialog, either:

   - if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or

   - if the request is routed elsewhere, create a Record-Route header containing its own SIP URI; and

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

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

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

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

3) execute the procedure described in step 4, 5, 6, 7, 8, 9, 10, 12 and 13 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

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

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), it shall:

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

2) insert a term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi;

2̶3)in the case where the S-CSCF has knowledge of an associated tel-URL for a SIP URI contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel-URL;

3̶4)in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header; and

4̶5)in case the response is sent towards the terminating user, the S-CSCF may remove the P-Access-Network-Info header based on local policy rules and the destination user (Request-URI).

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

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

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

2) insert a term-ioi parameter in the P-Charging-Vector header of the outgoing response. The S-CSCF shall set the term-ioi parameter to a value that identifies the sending network of the response and the orig-ioi parameter is set to the previously received value of orig-ioi.

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

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

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

3) create a Record-Route header containing its own SIP URI; and

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

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog (whether the user is registered or not), the S-CSCF shall:

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

2) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. In case the response is sent towards the terminating user, the S-CSCF may remove the header based on local policy rules and the destination user (Request-URI).

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

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

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

When the S-CSCF receives a response to a a subsequent request other than target refresh request for a dialog, in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. In case the response is sent towards the terminating user, the S-CSCF may remove the header based on local policy rules and the destination user (Request-URI).

*** next change ***

5.4.4 Call initiation

5.4.4.1 Initial INVITE

When the S-CSCF receives an INVITE request, either from the served user or destined to the served user, the S-CSCF may require the periodic refreshment of the session to avoid hung states in the S-CSCF. If the S-CSCF requires the session to be refreshed, it shall apply the procedures described in draft-ietf-sip-session-timer-12 [58] clause 8.

NOTE: Requesting the session to be refreshed requires support by at least one of the UEs. This functionality cannot automatically be granted, i.e. at least one of the involved UEs needs to support it.

5.4.4.2 Subsequent requests

5.4.4.2.1 Mobile-originating case

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

When the S-CSCF receives any 1xx or 2xx response, the S-CSCF shall insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

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

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

5.4.4.2.2 Mobile-terminating case

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

When the S-CSCF receives the any 1xx or 2xx response, the S-CSCF shall insert a P-Charging-Function-Addresses header populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS.

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

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

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **24.229** CR **724** | ⌘ **rev** | **1** | ⌘ | Current version: | **5.a.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:** | ⌘ | Request handling in S-CSCF originating case |

| **Source:** | ⌘ | Siemens |

| **Work item code:** | ⌘ | IMS-CCR | | **Date:** | ⌘ | 15/11/2004 |

| **Category:** | ⌘ | **F** | | **Release:** | ⌘ | Rel-5 |

Use <u>one</u> 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 <u>one</u> of the following releases:
Ph2　(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)
Rel-7　(Release 7)

| **Reason for change:** | ⌘ | Description of request handling in case requests are forwarded to AS(s) are ambigious. Ambigious condition when to store icid, when to insert orig-ioi, when to insert p-charging-funciton-address and when to add a second P-Asserted-Id. Requirment when to processing the request-URI is not defined |

| **Summary of change:** | ⌘ | See reason for change |

| **Consequences if not approved:** | ⌘ | Handling of requests with regards to applying filter criteria not possible. Ambigious handling of above mentioned parameters |

| **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.

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 header field of the request or not. In case the said header field 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;

NOTE 1: If the P-Asserted-Identity header field contains a barred public user identity, then the message has been received, either directly or indirectly, from a non-compliant entity which should have had generated the content with a non-barred public user identity.

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

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

4) check whether the initial request matches the next unexecuted initial filter criteria based on a public user identity in the P-Asserted-Identity header in the priority order as described in 3GPP TS 23.218 [5], and if it does, forward this request to that AS, 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 AS 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 AS(s) before processing the outgoing Request-URI. In case of contacting one or more AS(s) the S-CSCF shall:

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

NOTE 2: Depending on the result of processing the filter criteria the S-CSCF might contact one or more AS(s) before processing the outgoing Request URI.

5) if there is no original dialog identifier present in the topmost Route header of the incoming request 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) if there is no original dialog identifier present in the topmost Route header of the incoming request 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) if there is no original dialog identifier present in the topmost Route header of the incoming request 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) if there is no original dialog identifier present in the topmost Route header of the incoming request and if the S-CSCF has knowledge of an associated tel-URI for a SIP URI contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;

9) if the request is not forwarded to an AS and 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 URI using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator;

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

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

12) in case of an initial request for a dialog the S-CSCF shall create a Record-Route header containing its own SIP URI;

13) if the destination user (Request-URI) lies outside of the trust domain of the S-CSCF, remove the P-Access-Network-Info header, prior to forwarding the message;

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

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

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

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

NOTE 23: This header would normally only be expected in 1xx or 2xx responses.

NOTE 34: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3323 [33].

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response in order to be able to release the session if needed.

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

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

2) create a Record-Route header containing its own SIP URI;

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

4) in case the request is routed towards the destination user (Request-URI)or is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header; and

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

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed.

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

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

2) in case the request is routed towards the destination user (Request-URI)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.

CR-Form-v7.1

CHANGE REQUEST

⌘ **24.229 CR 725** ⌘ **rev 1** ⌘ Current version: **6.4.0** ⌘

*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: ⌘	Request handling in S-CSCF originating side	
Source: ⌘	Siemens	
Work item code: ⌘	IMS-CCR	***Date:*** ⌘ 15/11/2004
Category: ⌘ **A**		***Release:*** ⌘ Rel-6

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:
Ph2 *(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)*
Rel-7 *(Release 7)*

Reason for change: ⌘	Description of request handling in case requests are forwarded to AS(s) are ambigious. Ambigious condition when to store icid, when to insert orig-ioi, when to insert p-charging-funciton-address and when to add a second P-Asserted-Id. Requirment when to processing the request-URI is not defined
Summary of change: ⌘	See reason for change
Consequences if not approved: ⌘	Handling of requests with regards to applying filter criteria not possible. Ambigious handling of above mentioned parameters

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.

5.4.3 General treatment for all dialogs and standalone transactions excluding requests terminated by the S-CSCF

5.4.3.1 Determination of mobile-originated or mobile-terminated case

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

- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the request makes use of the information for mobile-originating calls, which was added to the Service-Route header entry of the S-CSCF during registration (see subclause 5.4.1.2), e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter; or,

- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the topmost Route header of the request contains the "orig" parameter. The S-CSCF shall remove the "orig" parameter from the topmost Route header; or,

- perform the procedures for the mobile-terminating case as described in subclause 5.4.3.3 if this information is not used by the request.

5.4.3.2 Requests initiated by the served user

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

Editor's Note: It needs to be stated, that the S-CSCF will only perform the following steps if the request was received from a trusted entity, e.g. an entity within the trust domain.

1) determine whether the request contains a barred public user identity in the P-Asserted-Identity header field of the request or not. In case the said header field 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;

NOTE 1: If the P-Asserted-Identity header field contains a barred public user identity, then the message has been received, either directly or indirectly, from a non-compliant entity which should have had generated the content with a non-barred public user identity.

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

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

4) check whether the initial request matches the next unexecuted initial filter criteria based on a public user identity in the P-Asserted-Identity header in the priority order as described in 3GPP TS 23.218 [5], and if it does, forward this request to that AS, 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 AS 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 AS(s) before processing the outgoing Request-URI. In case of contacting one or more AS(s) the S-CSCF shall:

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

   NOTE 2: Depending on the result of processing the filter criteria the S-CSCF might contact one or more AS(s) before processing the outgoing Request URI.

5) if there is no original dialog identifier present in the topmost Route header of the incoming request 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) if there is no original dialog identifier present in the topmost Route header of the incoming request 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) if there is no original dialog identifier present in the topmost Route header of the incoming request 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) if there is no original dialog identifier present in the topmost Route header of the incoming request and if~~in the case where~~ the S-CSCF has knowledge of an associated tel-URI for a SIP URI contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;

9) if the request is not forwarded to an AS and 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 URI using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [24]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or the S-CSCF may send an appropriate SIP response to the originator;

10) determine the destination address (e.g. DNS access) using the URI placed in the topmost Route header if present, otherwise based on the Request-URI. If the destination address is of an IP address type other than the IP address type used in the IM CN subsystem , then the S-CSCF shall forward the request to the IMS-ALG if the IM CN subsytem supports interworking to networks with different IP address type;

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 originated from a served user, either:

- if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or

- if the request is routed elsewhere, create a Record-Route header containing its own SIP URI;

NOTE ~~2~~3: For requests originated from a PSI the S-CSCF can decide whether to record-route or not.

Editor's Note: It needs to be clarified how the S-CSCF decides whether to put its address into the Record-Route header in the case of handling a request that originates from a PSI. It might be part of the operators policy.

13) based on local policy rules and the destination user (Request-URI), remove the P-Access-Network-Info header prior to forwarding the message;

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

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

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

1) apply any privacy required by RFC 3325 [34] to the P-Asserted-Identity header; and

2) apply the same privacy mechanism to the P-Access-Network-Info header, if present.

NOTE ~~3~~4: The P-Asserted-Identity header would normally only be expected in 1xx or 2xx responses.

NOTE ~~4~~5: The optional procedures above are in addition to any procedure for the application of privacy at the edge of the trust domain specified by RFC 3323 [33].

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response in order to be able to release the session if needed.

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

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

2) create a Record-Route header containing its own SIP URI;

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

4) in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header;

5) in case the request is routed towards the destination user (Request-URI) based on local policy rules and the destination user (Request-URI), remove the P-Access-Network-Info header; and

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

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog, if the response corresponds to an INVITE request, the S-CSCF shall save the Contact and Record-Route header field values in the response such that the S-CSCF is able to release the session if needed.

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

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

2) in case the request is routed to an AS located outside the trust domain, remove the P-Access-Network-Info header; and

3) in case the request is routed towards the destination user (Request-URI) based on local policy rules and the destination user (Request-URI), remove the P-access-network-info header; and

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

CR-Form-v7.1

CHANGE REQUEST

⌘	**24.229** CR **726**	⌘ **rev**	**1**	⌘	Current version:	**5.a.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: ⌘	Request handling in S-CSCF – terminating case	
Source: ⌘	Siemens	
Work item code:⌘	IMS-CCR	***Date:*** ⌘　15/11/2004
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:
　Ph2　　(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)
　Rel-7　(Release 7)

Reason for change: ⌘	On the reception of request, Ambigious condition when to insert a P-Charging-Funciton addr, when to store the ICID, when to store orig-ioi
Summary of change: ⌘	See above
Consequences if not approved: ⌘	Handling of mentioned headers above incorrect, charging tickets will be incorrect

Clauses affected: ⌘	5.4.3.3

	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.

5.4.3.3 Requests terminated at the served user

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

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

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

3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request.

   - If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request.

   - If not present, it indicates that the request is visiting the S-CSCF for the first time, and in this case the S-CSCF shall save the Request-URI from the request;

4) check whether the initial request matches the next unexecuted initial filter criteria in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

NOTE 1: Depending on the result of the previous process, the S-CSCF may contact one or more AS(s) before processing the outgoing Request-URI.

5) if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header field, if not present, populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

6) if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header;

7) if there is no original dialog identifier present in the topmost Route header of the incoming store the value of the orig-ioi parameter received in the P-Charging-Vector header, if present. The orig-ioi parameter identifies the sending network of the request message. The orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS;

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

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

   b) forward the request based on the Request-URI and skip the following steps;

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

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

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

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

   c) build a Request-URI with the contents of the saved Contact URI determined in the previous step; and

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

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

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

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].

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

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

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

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

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

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

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), it shall:

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

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

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

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

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

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

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

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

3) create a Record-Route header containing its own SIP URI; and

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

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog (whether the user is registered or not), the S-CSCF shall:

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

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

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

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

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

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

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **24.229** CR **727** | ⌘**rev** | **1** | ⌘ | Current version: | **6.4.0** | ⌘ |

*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:	⌘	Request handling in S-CSCF – terminating case
Source:	⌘	Siemens
Work item code:	⌘	IMS-CCR	**Date:** ⌘	15/11/2004
Category:	⌘	**A**	**Release:** ⌘	Rel-6

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:
Ph2 *(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)*
Rel-7 *(Release 7)*

| **Reason for change:** | ⌘ | On the reception of request, Ambigious condition when to insert a P-Charging-Funciton addr, when to store the ICID, when to store orig-ioi. Incorrect condition when to forward a request inc case the request is forked.
On the reception of INVITE for an unregistered user caller-prefs can not be performed. |

| **Summary of change:** | ⌘ | See above |

| **Consequences if not approved:** | ⌘ | Handling of mentioned headers above incorrect, charging tickets will be incorrect. Forking does not work. |

| **Clauses affected:** | ⌘ | 5.4.3.3 |

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

| **Other comments:** | ⌘ | |

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

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

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

## 5.4.3.3	Requests terminated at the served user

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

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

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

3)	check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request.

	-	If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request.

	-	If not present, it indicates that the request is visiting the S-CSCF for the first time, and in this case the S-CSCF shall save the Request-URI from the request;

4)	check whether the initial request matches the next unexecuted initial filter criteria in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

NOTE 1:	Depending on the result of the previous process, the S-CSCF may contact one or more AS(s) before processing the outgoing Request-URI.

5)	if there is no original dialog identifier present in the topmost Route header of the incoming request insert a P-Charging-Function-Addresses header field, if not present, populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

6)	if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the icid parameter received in the P-Charging-Vector header and retain the icid parameter in the P-Charging-Vector header;

7)	if there is no original dialog identifier present in the topmost Route header of the incoming request store the value of the orig-ioi parameter received in the P-Charging-Vector header, if present. The orig-ioi parameter identifies the sending network of the request message. The orig-ioi parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AS;

8)	if necessary perform the caller preferences to callee capabilities matching according to draft-ietf-sip-caller-preferences [62];

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

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

	b)	forward the request based on the Request-URI and skip the following steps;

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

9)	if necessary perform the caller preferences to callee capabilities matching according to draft-ietf-sip-caller-preferences [62];

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

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

b) determine, from the destination public user identity, the saved Contact URI where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2. If there is more than one contact address saved for the destination public user identity, the S-CSCF shall:

- if the fork directive in the Request Disposition header was set to "no-fork", ~~forward the request to~~ the contact with the highest qvalue parameter shall be used when building the Request-URI. In case no qvalue parameters were provided, the S-CSCF shall decide locally ~~how to forward the request~~what contact address to be used when building the Request-URI; otherwise

- fork the request or perform sequential search based on the relative preference indicated by the qvalue parameter of the Contact header in the original REGISTER request, as described in RFC3261 [26]. In case no qvalue parameters were provided, then the S-CSCF shall ~~forward the request as~~determine the contact address to be used when building the Request-URI as directed by the Request Disposition header as described in draft-ietf-sip-callerprefs-10 [56B]. If the Request-Disposition header is not present, the S-CSCF shall decide locally whether to fork or perform sequential search among the contact addresses;

c) build a Request-URI with the contents of the saved Contact URI determined in the previous step; and

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

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

12) optionally, apply any privacy required by RFC 3325 [34] to the P-Asserted-Identity header and apply the same privacy mechanism to the P-Access-Network-Info header;

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].

13) in case of an initial request for a dialog, either:

- if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or

- if the request is routed elsewhere, create a Record-Route header containing its own SIP URI; and

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

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

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

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

3) execute the procedure described in step 4, 5, 6, 7, 8, ~~9~~, 10, 12 and 13 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

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

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), it shall:

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

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

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

4) in case the response is sent towards the ~~terminating~~ orignating user, the S-CSCF may remove the P-Access-Network-Info header based on local policy rules and the destination user (Request-URI).

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

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

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

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

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

3) create a Record-Route header containing its own SIP URI; and

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

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog (whether the user is registered or not), the S-CSCF shall:

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

2) in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. In case the response is sent towards the ~~terminating~~ originating user, the S-CSCF may remove the header based on local policy rules and the destination user (Request-URI).

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

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

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

When the S-CSCF receives a response to a a subsequent request other than target refresh request for a dialog, in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. In case the response is sent towards the terminating user, the S-CSCF may remove the header based on local policy rules and the destination user (Request-URI).

3GPP TSG–CN1 Meeting #36

Seoul, Korea, 15ᵗʰ to 19ᵗʰ November 2004

Tdoc ⌘**N1-041961**

CR-Form-v7

CHANGE REQUEST

⌘	**24.229**	CR	**737**	⌘ **rev**	**1**	⌘	Current version:	**5.10.0**	⌘

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:	⌘	Population of Via header when using REGISTER method
Source:	⌘	Vodafone

Work item code:	⌘	IMS-CCR		**Date:** ⌘	04/11/2004

Category: ⌘ **F**

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

Release: ⌘ Rel-5

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	Including the protected server port value within the Via and Contact header for the generic procedures applicable to all methods excluding the REGISTER method is given in Subclause 5.1.2A. Furthermore, how to populate the protected server port value within the Contact header for the initial registration, the user-initiated re-registration and the user-initiated de-registration procedures using REGISTER method is given in Subclause 5.1.1.2, 5.1.1.4 and 5.1.1.6, respectively. However, it is not specified in those subclauses how to handle the protected server port value within the Via header.
Summary of change:	⌘	Conditional including the protected server port value in the Via header is added in Subclause 5.1.1.2

Populating the protected server port value within the Via header is added in Subclauses 5.1.1.4 and 5.1.1.6, respectively.

Editorial change in Subclause 5.1.1.6. |
| **Consequences if not approved:** | ⌘ | Incomplete specification may lead to different UE implementations when populating the protected server port value within the Via header on sending REGISTER request. |

Clauses affected:	⌘	5.1.1.2; 5.1.1.4; 5.1.1.6

		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.

<div style="text-align:center; border:1px solid;">*** FIRST CHANGE ***</div>

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 protected using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration.

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. 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 REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;

e)   the Via header containing the IP address or FQDN of the UE in the ~~hostport parameter~~sent-by field ~~or FQDN~~. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the ~~hostport parameter~~sent-by field.

NOTE 1:   If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via 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.

NOTE 2:   The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

f~~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 3:   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.

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

h~~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. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];

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

j~~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).

<div style="text-align:center; border:1px solid;">*** END OF FIRST CHANGE ***</div>

<div style="text-align:center">*** SECOND CHANGE ***</div>

5.1.1.4   User-initiated re-registration

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

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less. The UE shall protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if IK is available.

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 sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

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

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

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

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

e) a Via header containing the IP address or FQDN of the UE in the ~~hostport parameter~~ sent-by field ~~or FQDN~~ and the protected server port value bound to the security association;

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via 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.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

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

NOTE 3~~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.

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

h~~g~~) a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

i~~h~~) a Security-Verify header that contains the content of the Security-Server header received in the 401 (Unauthorized) response of the last successful authentication;

j~~i~~) the Supported header containing the option tag "path"; and

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

<div style="text-align:center">*** END OF SECOND CHANGE ***</div>

*** LAST CHANGE ***

5.1.1.6   ~~Mobile~~User-initiated deregistration

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

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

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.

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

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

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

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

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

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

  e)   a Via header containing the IP address or FQDN of the UE in the ~~hostport parameter~~sent-by field ~~or FQDN~~ and the protected server port value bound to the security association;

  NOTE 1:   If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via 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.

  f~~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;

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

  h~~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).

*** END OF LAST CHANGE ***

3GPP TSG–CN1 Meeting #36   *Tdoc* ⌘**N1-041962**
Seoul, Korea, 15ᵗʰ to 19ᵗʰ November 2004

CR-Form-v7

CHANGE REQUEST

| ⌘ | **24.229** CR **738** | ⌘ **rev** | **1** | ⌘ | Current version: | **6.4.0** | ⌘ |

*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: ⌘	Population of Via header when using REGISTER method		
Source: ⌘	Vodafone		
Work item code: ⌘	IMS-CCR	**Date:** ⌘	04/11/2004
Category: ⌘ **A**		**Release:** ⌘	Rel-6

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)
Rel-7   (Release 7)

Reason for change: ⌘	Including the protected server port value within the Via and Contact header for the generic procedures applicable to all methods excluding the REGISTER method is given in Subclause 5.1.2A. Furthermore, how to populate the protected server port value within the Contact header for the initial registration, the user-initiated re-registration and the user-initiated de-registration procedures using REGISTER method is given in Subclause 5.1.1.2, 5.1.1.4 and 5.1.1.6, respectively. However, it is not specified in those subclauses how to handle the protected server port value within the Via header.
Summary of change: ⌘	Conditional including the protected server port value in the Via header is added in Subclause 5.1.1.2 Populating the protected server port value within the Via header is added in Subclauses 5.1.1.4 and 5.1.1.6, respectively. Editorial change in Subclause 5.1.1.6.
Consequences if not approved: ⌘	Incomplete specification may lead to different UE implementations when populating the protected server port value within the Via header on sending REGISTER request.

Clauses affected: ⌘	5.1.1.2; 5.1.1.4; 5.1.1.6

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

Other comments: ⌘	

How to create CRs using this form:

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

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

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

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

*** FIRST CHANGE ***

5.1.1.2 Initial registration

The UE can register a public user identity with its contact address at any time after it has aquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. 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 protected using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration.

The UE shall extract or derive 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. 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 REGISTER request is protected by a security association, the UE shall also include the protected server port value in the hostport parameter;

e) the Via header containing the IP address or FQDN of the UE in the ~~hostport parameter~~sent-by field ~~or FQDN~~. If the REGISTER request is protected by a security association, the UE shall also include the protected server port value in the ~~hostport parameter~~sent-by field.

NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via 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.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

f~~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 3: 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.

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

h~~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. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203 [19]. The syntax of the parameters needed for the security association setup is specified in Annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the HMAC-MD5-96 (RFC 2403 [20C]) and HMAC-SHA-1-96 (RFC 2404 [20D]) IPsec layer algorithms, and shall announce support for them according to the procedures defined in RFC 3329 [48];

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

j~~i~~) if a security association exists, a P-Access-Network-Info header set as specified for the access network technology (for GPRS see subclause B.3).

*** END OF FIRST CHANGE ***

*** SECOND CHANGE ***

5.1.1.4   User-initiated re-registration

The UE can reregister a previously registered public user identity with its contact address at any time.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister the public user identity either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less. The UE shall protect the REGISTER request using a security association, see 3GPP TS 33.203 [19], established as a result of an earlier registration, if IK is available.

The UE shall extract or derive 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 sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

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

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

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

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

   e) a Via header containing the IP address or FQDN of the UE in the ~~hostport parameter~~sent-by field ~~or FQDN~~ and the protected server port value bound to the security association;

   NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via 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.

   NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

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

   NOTE 3: 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.

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

   h~~g~~)a Security-Client header field, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48];

   i~~h~~) a Security-Verify header that contains the content of the Security-Server header received in the 401 (Unauthorized) response of the last successful authentication;

   j~~i~~) the Supported header containing the option tag "path"; and

   k~~j~~) the P-Access-Network-Info header set as specified for the access network technology (for GPRS see subclause B.3).

*** END OF SECOND CHANGE ***

5.1.1.6   ~~Mobile~~User-initiated deregistration

The UE can deregister a public user identity that it has previously registered with its contact address at any time.

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

The UE shall extract or derive 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.

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

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

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

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

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

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

e) a Via header containing the IP address or FQDN of the UE in the ~~hostport parameter~~sent-by field ~~or FQDN~~ and the protected server port value bound to the security association;

   NOTE 1: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via 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~~f) 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;

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

~~h~~g) a P-Access-Network-Info header set as specified for the access network technology (for GPRS see subclause B.3).

3GPP TSG–CN1 Meeting #36   *Tdoc* ⌘**N1-041965**
Seoul, Korea, 15ᵗʰ to 19ᵗʰ November 2004

CR-Form-v7

CHANGE REQUEST

| ⌘ | **24.229** CR **764** | ⌘**rev** | **1** | ⌘ | Current version: | **5.10.0** | ⌘ |

*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:	⌘	Interaction between S-CSCF and HSS in Network initiated deregistration procedure

Source:	⌘	Orange

Work item code: ⌘	IMS-CCR		**Date:** ⌘	16/11/2004

Category:	⌘	**F**		**Release:** ⌘	Rel-5

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

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

Reason for change:	⌘	**It is an essential correction.**

Currently, the network initiated deregistration procedure does not clearly distinguish the case when the de-registration is initiated by the S-CSCF or by the HSS. Consequently, the interactions between the S-CSCF and HSS are not clearly stated.

In TS 23.228 section 5.3.2., it is required that:

- for an HSS initiated de-registration, the Cx-Deregister procedure applies (Cx-Deregister message sent by the HSS to the S-CSCF);

- for a S-CSCF initiated de-registration, the Cx-Put procedure applies (Cx-Put message sent by the S-CSCF to the HSS);

In case of HSS initiated de-registration (Cx-Deregister), it is required that the S-CSCF clears the registration and user information.

In case of S-CSCF initiated de-registration (Cx-Put), the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber and the S-CSCF either keep or remove the user information.

In TS 29.228, Cx-Deregister and Cx-Put respectively refer to Registration-Termination and Server-Assignment messages.

Summary of change: ⌘	In section 5.4.1.5, it is mentioned that:

- In case of HSS initiated de-registration, the S-CSCF shall respond to the HSS using the Cx Registration-Termination procedure with the HSS, as

	described in 3GPP TS 29.228; For this case, the S-CSCF shall remove those public user identities, their registration state and the associated service profiles from the local data.
	- In case of S-CSCF initiated de-registration, the S-CSCF shall deregister those public user identities and the associated implicitly registered public user identities using the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.228.
	Reference is made to TS 29.228 instead of TS 29.229 for the Cx procedures.
Consequences if not approved: ⌘	The case of HSS initiated deregistration is not covered in the network-initiated de-registration procedure.

Clauses affected: ⌘	5.4.1.5		
	Y	**N**	
Other specs affected: ⌘	**X**		Other core specifications ⌘ TS 24.228 (CR#136)
		X	Test specifications
		X	O&M Specifications
Other comments: ⌘	Mirror CR in R6		

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 co

5.4.1.5 Network-initiated deregistration

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

When a network-initiated deregistration event occurs for one or more public user identity, the S-CSCF shall send a NOTIFY request to all subscribers that have subscribed to the respective reg event package. Prior to sending the NOTIFY request, the S-CSCF shall release all sessions related to the public user identity being deregistered, if any. For each NOTIFY request, the S-CSCF shall:

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

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

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

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

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

   b) if the public user identity:

      i) has been deregistered then:

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

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

         - set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

      ii) has been kept registered then:

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

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

5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17].

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

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

On completion of the above procedures in this subclause for one or more public user identities, the S-CSCF shall deregister those public user identities and the associated implicitly registered public user identities. On completion of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.2298 [154], the S-CSCF shall update or remove those public user identities, their registration state and the associated service profiles from the local data (based on operators' policy the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber). On the completion of the Cx Registration-Termination procedure with the HSS, as described in 3GPP TS 29.228 [14], the S-CSCF shall remove those public user identities, their registration state and the associated service profiles from the local data.

> Editor's note: this procedure shall be improved for the case of de-registration of the old contact information when the UE is roaming, registration is done in a new network and the previous registration has not expired.

3GPP TSG–CN1 Meeting #36   *Tdoc* ⌘**N1-041966**
Seoul, Korea, 15th to 19th November 2004

CR-Form-v7
CHANGE REQUEST
⌘   **24.229** CR **765**   ⌘**rev** **1** ⌘   Current version: **6.4.0** ⌘

*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: ⌘	Interaction between S-CSCF and HSS in Network initiated deregistration procedure
Source: ⌘	Orange
Work item code:⌘	IMS-CCR ***Date:*** ⌘ 16/11/2004
Category: ⌘	**A** ***Release:*** ⌘ Rel-6

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

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

Reason for change: ⌘	**It is an essential correction.**
	Currently, the network initiated deregistration procedure does not clearly distinguish the case when the de-registration is initiated by the S-CSCF or by the HSS. Consequently, the interactions between the S-CSCF and HSS are not clearly stated.
	In TS 23.228 section 5.3.2., it is required that:
	- for an HSS initiated de-registration, the Cx-Deregister procedure applies (Cx-Deregister message sent by the HSS to the S-CSCF);
	- for a S-CSCF initiated de-registration, the Cx-Put procedure applies (Cx-Put message sent by the S-CSCF to the HSS);
	In case of HSS initiated de-registration (Cx-Deregister), it is required that the S-CSCF clears the registration and user information.
	In case of S-CSCF initiated de-registration (Cx-Put), the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber and the S-CSCF either keep or remove the user information.
	In TS 29.228, Cx-Deregister and Cx-Put respectively refer to Registration-Termination and Server-Assignment messages.
Summary of change: ⌘	In section 5.4.1.5, it is mentioned that:
	- In case of HSS initiated de-registration, the S-CSCF shall respond to the HSS using the Cx Registration-Termination procedure with the HSS, as

		described in 3GPP TS 29.228; For this case, the S-CSCF shall remove those public user identities, their registration state and the associated service profiles from the local data.
	-	In case of S-CSCF initiated de-registration, the S-CSCF shall deregister those public user identities and the associated implicitly registered public user identities using the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.228.
		Reference is made to TS 29.228 instead of TS 29.229 for the Cx procedures.
Consequences if not approved:	⌘	The case of HSS initiated deregistration is not covered in the network-initiated de-registration procedure.

Clauses affected:	⌘	5.4.1.5			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

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

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

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

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause co

5.4.1.5 Network-initiated deregistration

NOTE 1: A network-initiated deregistration event that occurs at the S-CSCF may be received from the HSS or may be an internal event in the S-CSCF.

Prior to initiating the network-initiated deregistration for the only currently registered public user identity and its associated set of implicitly registered public user identities that have been registered with the same contact (i.e. no other public user identity is registered with this contact) while there are still active multimedia sessions belonging to this contact, the S-CSCF shall release only the multimedia sessions belonging to this contact as described in subclause 5.4.5.1. The multimedia sessions for the same public user identity, if registered with another contact remain unchanged.

When a network-initiated deregistration event occurs for one or more public user identities that are bound to one or more contacts, the S-CSCF shall send a NOTIFY request to all subscribers that have subscribed to the respective reg event package. Prior to sending the NOTIFY request, the S-CSCF may release all sessions related to the contacts that will be deregistered. For each NOTIFY request, the S-CSCF shall:

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

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

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

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

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

   b) if the public user identity:

      i) has been deregistered then:

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

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

         - set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

      ii) has been kept registered then:

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

         II) set the state attribute within the <contact> element to:

            - for the contact address to be removed set the state attribute within the <contact> element to "terminated", and event attribute element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

            - for the contact address which remain unchanged, if any, leave the <contact> element unmodified; and

NOTE 2: There might be more then one contact information available for one public user identity. When deregistering this UE, the S-CSCF will only modify the <contact> elements that were originally registered by this UE using its private user identity. The <contact> elements of the same public user identity, if registered by another UE using different private user identities remain unchanged.

5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.260 [17].

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

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

On completion of the above procedures for one or more public user identities, the S-CSCF shall deregister those public user identities and the associated implicitly registered public user identities. On completion of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.2298 [154], the S-CSCF shall update or remove those public user identities, their registration state and the associated service profiles from the local data (based on operators' policy the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber). On the completion of the Cx Registration-Termination procedure with the HSS, as described in 3GPP TS 29.228 [14], the S-CSCF shall remove those public user identities, their registration state and the associated service profiles from the local data.

Editor's note: this procedure shall be improved for the case of deregistration of the old contact information when the UE is roaming, registration is done in a new network and the previous registration has not expired and the case of de-registration of a contact information when multiple UEs are using the same public user identity and one of these UEs is deregistered.

*** END OF MODIFICATION ***

3GPP TSG–CN1 Meeting #36   *Tdoc* ⌘**N1-041967**
Seoul, Korea, 15th to 19th November 2004

CR-Form-v7

CHANGE REQUEST

⌘	**24.228** CR **136**	⌘**rev**		⌘	Current version:	**5.10.0** ⌘

*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:	⌘	Interaction between S-CSCF and HSS in Network initiated deregistration procedure
Source:	⌘	Orange
Work item code:⌘	IMS-CCR	**Date:** ⌘ 16/11/2004

Category:	⌘	**F**	**Release:** ⌘ Rel-5

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

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

Reason for change:	⌘	**It is an essential correction.**

Currently, the interactions between the S-CSCF and HSS are not correctly stated in case a network initiated de-registration is initiated by the S-CSCF.

In TS 24.229 section 5.4.1.5, the UE and P-CSCF notifications are performed before the S-CSCF does the Cx-Server-Assignment procedure (S-CSCF deregistration notification).

Summary of change:⌘ In section 6.7, the S-CSCF de-registration notification is moved from step 2 to last step.

Consequences if ⌘ Inconsistency with the procedure described in TS 24.229.
not approved:

Clauses affected: ⌘ 6.7.1

	Y	**N**			
Other specs ⌘	**X**		Other core specifications	⌘	TS 24.229 (CR#764)
affected:		**X**	Test specifications		
		X	O&M Specifications		

Other comments: ⌘

How to create CRs using this form:

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

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

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

3)With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause co

*** FIRST MODIFICATION ***

6.7.1 Network-initiated deregistration event occurs in the S-CSCF

Figure 6.7.1-1 assumes that the UE and the P-CSCF both have subscribed for the user's registration state event package according to subclause 6.5 and shows how the UE and the P-CSCF are notified when the network-initiated deregistration event occurs in the S-CSCF.

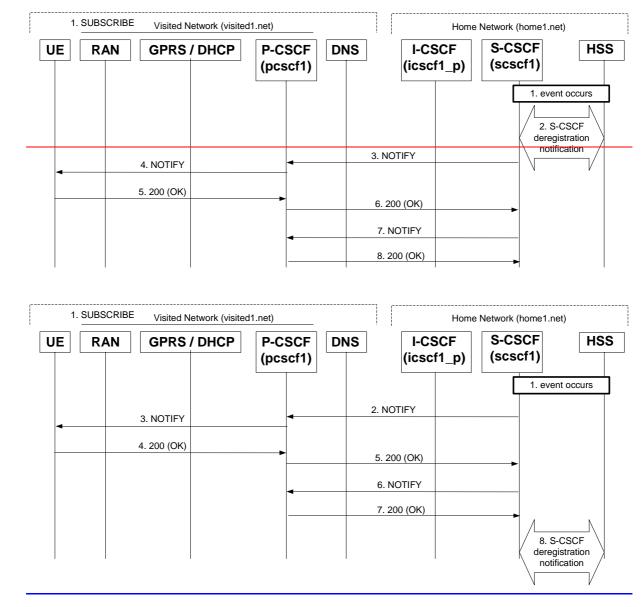Also, it is assumed that the home network does not have network configuration hiding active.

Figure 6.7.1-1: Network Initiated Deregistration event occurs in the S-CSCF

1. **Network Initiated Deregistration event occurs in the S-CSCF**

2. ~~**S-CSCF deregistration notification**~~

~~When the Network Initiated Deregistration Event occurs in the S-CSCF, the S-CSCF informs the HSS that the user is no longer registered. The S-CSCF either notifies the HSS to clear or requests to keep its location information for that subscriber. The HSS then either clears or keeps the S-CSCF name for that subscriber according to request. In both cases the state of the subscriber identity is stored as unregistered in the HSS and the S-CSCF. The HSS acknowledges the request.~~

~~For detailed message flows see 3GPP TS 29.228 [11].~~

~~3~~2 **SIP NOTIFY request (S-CSCF to P-CSCF) - see example in table 6.7.1-3**

After the S-CSCF deregistration notification procedure the S-CSCF immediately sends a NOTIFY request towards the UE in order to inform about the network initiated deregistration and the subscription termination. The same Request URI, To, From, Call-ID are used as in the first NOTIFY request. CSeq is incremented since this is the second NOTIFY request sent towards the UE.

Table 6.7.1-3: SIP NOTIFY request (S-CSCF to P-CSCF)

```
NOTIFY sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1
Max-Forwards: 70
Route: <sip:pcscf1.visited1.net;lr>
From: <sip:user1_public1@home1.net>;tag=151170
To: <sip:user1_public1@home1.net>;tag=31415
Call-ID: b89rjhnedlrfjflslj40a222
CSeq: 43 NOTIFY
Subscription-State: terminated
Event: reg
Content-Type: application/reginfo+xml
Contact: sip:scscf1.home1.net
Content-Length: (...)

<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
                version="1" state="full">
    <registration aor="sip:user1_public1@home1.net" id="as9"
                state="terminated">
      <contact id="76" state="terminated" event="deactivated">
         <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
      </contact>
    </registration>
    <registration aor="sip:user1_public2@home1.net" id="as10"
                state="terminated">
      <contact id="77" state="terminated" event="deactivated">
         <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
      </contact>
    </registration>
    <registration aor="tel:+358504821437" id="as11"
                state="terminated">
      <contact id="78" state="terminated" event="deactivated">
         <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
      </contact>
    </registration>
  </reginfo>
```

~~4~~3. **SIP NOTIFY request (P-CSCF to UE) - see example in table 6.7.1-4**

P-CSCF forwards the NOTIFY request to the UE.

Table 6.7.1-4: SIP NOTIFY request (P-CSCF to UE)

```
NOTIFY sip:[5555::aaa:bbb:ccc:ddd]:1357;comp=sigcomp SIP/2.0
Via: SIP/2.0/UDP pcscf1.visited1.net:7531;comp=sigcomp;branch=z9hG4bK240f34.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1
Max-Forwards: 69
From:
To:
Call-ID:
CSeq:
Subscription-State:
Event:
Content-Type:
Contact:
Content-Length:
```

~~5~~4. **200 (OK) response (UE to P-CSCF) - see example in table 6.7.1-5**

Table 6.7.1-5: SIP 200 (OK) response (UE to P-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP pcscf1.visited1.net:7531;comp=sigcomp;branch=z9hG4bK240f34.1, SIP/2.0/UDP
scscf1.home1.net;branch=z9hG4bK332b23.1
```

```
P-Access-Network-Info: 3GPP-UTRAN-TDD; utran-cell-id-3gpp=234151D0FCE11
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

P-Access-Network-Info: the UE provides the access-type and access-info, related to the serving access network.

~~6~~5. **SIP 200 (OK) response (P-CSCF to S-CSCF) - see example in table 6.7.1-6**

Table 6.7.1-6: SIP 200 (OK) response (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1
P-Access-Network-Info:
From:
To:
Call-ID:
CSeq:
Content-Length:
```

P-Access-Network-Info: This header contains information from the UE.

~~7~~6 **SIP NOTIFY request (S-CSCF to P-CSCF) - see example in table 6.7.1-7**

The S-CSCF also sends a NOTIFY request towards the P-CSCF to which the UE is attached to, in order to inform about the network initiated deregistration. The same Request URI, To, From, Call-ID are used as in the first NOTIFY request. CSeq is incremented since this is the second NOTIFY request sent towards the P-CSCF.

Table 6.7.1-7: SIP NOTIFY request (S-CSCF to P-CSCF)

```
NOTIFY sip:pcscf1.visited1.net SIP/2.0
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1
Max-Forwards: 70
From: <sip:user1_public1@home1.net>;tag=151170
To: <sip:pcscf1.visited1.net>;tag=31415
Call-ID: dre36d2v32gnlgiiomm72445
CSeq: 43 NOTIFY
Subscription-State: terminated
Event: reg
Content-Type: application/reginfo+xml
Contact: sip:scscf1.home1.net
Content-Length: (...)

<?xml version="1.0"?>
<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"
              version="1" state="full">
    <registration aor="sip:user1_public1@home1.net" id="as9"
                state="terminated">
     <contact id="76" state="terminated" event="deactivated">
        <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
      </contact>
    </registration>
    <registration aor="sip:user1_public2@home1.net" id="as10"
                state="terminated">
     <contact id="77" state="terminated" event="deactivated">
        <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
      </contact>
    </registration>
    <registration aor="tel:+358504821437" id="as11"
                state="terminated">
     <contact id="78" state="terminated" event="deactivated">
        <uri>sip:[5555::aaa:bbb:ccc:ddd]</uri>
      </contact>
    </registration>
   </reginfo>
```

~~8~~7. **SIP 200 (OK) response (P-CSCF to S-CSCF) - see example in table 6.7.1-8**

Table 6.7.1-8: SIP 200 (OK) response (P-CSCF to S-CSCF)

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP scscf1.home1.net;branch=z9hG4bK332b23.1
From:
To:
Call-ID:
CSeq:
Content-Length: 0
```

8. **S-CSCF deregistration notification**

When the Network Initiated Deregistration Event occurs in the S-CSCF, the S-CSCF informs the HSS that the user is no longer registered. The S-CSCF either notifies the HSS to clear or requests to keep its location information for that subscriber. The HSS then either clears or keeps the S-CSCF name for that subscriber according to request. In both cases the state of the subscriber identity is stored as unregistered in the HSS and the S-CSCF. The HSS acknowledges the request.

For detailed message flows see 3GPP TS 29.228 [11].

*** END OF MODIFICATION ***

CR-Form-v7

CHANGE REQUEST

⌘	**24.229** CR **754**	⌘**rev**	**1**	⌘	Current version:	**5.10.0** ⌘

*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:	⌘	Network-initiated deregistration for the old contact information of a roaming UE registered in a new network

Source:	⌘	Orange

Work item code:⌘	IMS-CCR		**Date:** ⌘	20/11/2004

Category:	⌘	**F**		**Release:** ⌘	Rel-5

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

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

Reason for change:	⌘	When the UE is roaming, registration is done in a new network using a new contact address and the previous registration has not expired, the old contact shall be deregistered but not the new contact. The procedure should be improved to handle this case in section 5.4.1.5.

Summary of change:⌘		The text in section 5.4.1.5 is modified so that the specific case of deregistration of the old contact information when a UE is roaming, registration is done in a new network (i.e. using a new contact address and the previous registration has not expired) is added.
		In section 5.4.1.2, a reference is added to the new subclause 5.4.1.5.

Consequences if not approved:	⌘	Incorrect handling in the case of deregistration of the old contact information when the UE is roaming, registration is done in a new network and the previous registration has not expired.

Clauses affected:	⌘	5.4.1.2, 5.4.1.5

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

Other comments:	⌘	

How to create CRs using this form:

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

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

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

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause co

5.4.1.2 Initial registration and user-initiated reregistration

5.4.1.2.1 Unprotected REGISTER

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

NOTE 2: A REGISTER with Expires header value equal to zero should always be received protected. However, it is possible that in error conditions a REGISTER with Expires header value equal to zero may be received unprotected. In that instance the procedures below will be applied.

When the S-CSCF receives a new unprotected registration request for an already registered public user identity linked to the same private user identity but with a new contact information (e.g. a user roams to a different network without de-registering the previous one), the S-CSCF shall:

> 1) perform the procedure for 'receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no"', for the received public user identity; and

> 2) if the authentication has been successful and if the previous registration has not expired, the S-CSCF shall perform the network initiated de-registration procedure only for the previous contact information as described in subclause 5.4.1.5.4.

Upon receipt of a REGISTER request without an "integrity-protected" parameter, or with the "integrity-protected" parameter in the Authorization header set to "no", the S-CSCF shall:

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

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

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

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

NOTE 3: At this point the S-CSCF informs the HSS, that the user currently registering will be served by the S-CSCF by passing its SIP URI to the HSS. This will be indicated by the HSS for all further incoming requests to this user, in order to direct all these requests directly to this S-CSCF.

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

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

- the home network identification in the realm field;

- the RAND and AUTN parameters and optional server specific data for the UE in the nonce field;

- the security mechanism, which is AKAv1-MD5, in the algorithm field;

- the IK (Integrity Key) parameter for the P-CSCF in the ik field (see subclause 7.2A.1); and

- the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2A.1);

6) store the RAND parameter used in the 401 (Unauthorized) response for future use in case of a resynchronisation. If a stored RAND already exists in the S-CSCF, the S-CSCF shall overwrite the stored RAND with the RAND used in the most recent 401 (Unauthorized) response;

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

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

If the received REGISTER request indicates that the challenge sent previously by the S-CSCF to the UE was deemed to be invalid by the UE, the S-CSCF shall stop the timer reg-await-auth and proceed as described in the subclause 5.4.1.2.3.

<div style="border:1px solid black; text-align:center">*** END OF FIRST MODIFICATION ***</div>

<div style="border:1px solid black; text-align:center">*** SECOND MODIFICATION ***</div>

5.4.1.5   Network-initiated deregistration

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

When a network-initiated deregistration event occurs for one or more public user identity, the S-CSCF shall send a NOTIFY request to all subscribers that have subscribed to the respective reg event package. Prior to sending the NOTIFY request, the S-CSCF shall release all sessions related to the public user identity being deregistered, if any. For each NOTIFY request, the S-CSCF shall:

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

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

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

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

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

    b) if the public user identity:

        i) has been deregistered then:

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

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

            -   set the event attribute within the <contact> element to "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

        ii) has been kept registered then:

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

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

5) add a P-Charging-Vector header with the icid parameter populated as specified in 3GPP TS 32.225 [17].

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

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

In case of the deregistration of the old contact information when the UE is roaming, registration is done in a new network and the previous registration has not expired, on completion of the above procedures, the S-CSCF shall remove the registration information related to the old contact from the local data.

Otherwise, ~~O~~on completion of the above procedures in this subclause for one or more public user identities, the S-CSCF shall deregister those public user identities and the associated implicitly registered public user identities. On completion of the Cx Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [15], the S-CSCF shall update or remove those public user identities, their registration state and the associated service profiles from the local data (based on operators' policy the S-CSCF can request of the HSS to either be kept or cleared as the S-CSCF allocated to this subscriber).

~~Editor's note: this procedure shall be improved for the case of de-registration of the old contact information when the UE is roaming, registration is done in a new network and the previous registration has not expired.~~

*** END OF SECOND MODIFICATION ***

3GPP TSG–CN1 Meeting #36
Seoul, Korea, 15th to 19th November 2004

Tdoc ⌘**N1-042102**

CR-Form-v7

CHANGE REQUEST

| ⌘ | **24.229** CR **767** | ⌘**rev** | **1** | ⌘ | Current version: | **5.10.0** | ⌘ |

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: ⌘	Downloading of user profile		
Source: ⌘	Orange		
Work item code: ⌘	IMS-CCR	***Date:*** ⌘	20/11/2004
Category: ⌘ **F**		***Release:*** ⌘	Rel-5

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

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

Reason for change: ⌘	**It is an essential correction.**
	Currently, the treatment of incoming initial requests at the terminating S-CSCF is distinguished according to the user registration state. However, in both cases, the first step consists in verifying that the "Request-URI" of the request is not barred.
	For the registered state, the user profile is stored at the HSS at the end of the registration procedure.
	For the unregistered state, in case the called party is in this state due to a terminating call when the user has services related to the unregistered state, the user profile may be not present yet when the terminating S-CSCF receives e.g. an initial request for a dialog. For that reason, the S-CSCF is not able to determine whether the destination is barred or not. That is why the S-CSCF should download the user profile if not present before exceuting the first step of the current procedure.
Summary of change: ⌘	In section 5.4.3.3 in the paragraph detailing the behaviour of the terminating S-CSCF for a request destinated to an unregistered user, it is proposed to reverse 1) and 2) so that the S-CSCF firstly stores the user profile if not present before examining whether the destination of the request is barred or not.
Consequences if not approved: ⌘	Inconsistent sequence of current treatment at the terminating S-CSCF for an unregistered user

Clauses affected:	⌘	5.4.3.3		

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

Other comments:	⌘	Mirror CR in R6

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 co

5.4.3.3   Requests terminated at the served user

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

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

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

3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request.

   - If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request.

   - If not present, it indicates that the request is visiting the S-CSCF for the first time, and in this case the S-CSCF shall save the Request-URI from the request;

4) check whether the initial request matches the next unexecuted initial filter criteria in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

NOTE 1: Depending on the result of the previous process, the S-CSCF may contact one or more AS(s) before processing the outgoing Request-URI.

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

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

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

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

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

   b) forward the request based on the Request-URI and skip the following steps;

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

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

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

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

   c) build a Request-URI with the contents of the saved Contact URI determined in the previous step; and

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

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

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

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].

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

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

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

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

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

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

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

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), it shall:

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

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

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

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

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

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

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

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

3) create a Record-Route header containing its own SIP URI; and

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

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog (whether the user is registered or not), the S-CSCF shall:

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

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

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

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

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

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

*** END OF MODIFICATION ***

3GPP TSG–CN1 Meeting #36   *Tdoc* ⌘N1-042103
Seoul, Korea, 15ᵗʰ to 19ᵗʰ November 2004

CR-Form-v7

CHANGE REQUEST

⌘	**24.229**	CR	**768**	⌘ **rev**	**1**	⌘	Current version:	**6.4.0**	⌘

*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:	⌘	Downloading of user profile	
Source:	⌘	Orange	
Work item code:⌘	IMS-CCR	***Date:*** ⌘	20/11/2004

Category:	⌘ **A**	***Release:*** ⌘	Rel-6

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

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

Reason for change: ⌘	**It is an essential correction.**
	Currently, the treatment of incoming initial requests at the terminating S-CSCF is distinguished according to the user registration state. However, in both cases, the first step consists in verifying that the "Request-URI" of the request is not barred.
	For the registered state, the user profile is stored at the HSS at the end of the registration procedure.
	For the unregistered state, in case the called party is in this state due to a terminating call when the user has services related to the unregistered state, the user profile may be not present yet when the terminating S-CSCF receives e.g. an initial request for a dialog. For that reason, the S-CSCF is not able to determine whether the destination is barred or not. That is why the S-CSCF should download the user profile if not present before exceuting the first step of the current procedure.

Summary of change: ⌘	In section 5.4.3.3 in the paragraph detailing the behaviour of the terminating S-CSCF for a request destinated to an unregistered user, it is proposed to reverse 1) and 2) so that the S-CSCF firstly stores the user profile if not present before examining whether the destination of the request is barred or not.

Consequences if not approved:	⌘ Inconsistent sequence of current treatment at the terminating S-CSCF for an unregistered user

Clauses affected:	⌘	5.4.3.3			

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

Other comments:	⌘	

How to create CRs using this form:

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

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

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

3)With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause co

5.4.3.3 Requests terminated at the served user

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

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

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

3) check if an original dialog identifier that the S-CSCF previously placed in a Route header is present in the topmost Route header of the incoming request.

   - If present, it indicates an association with an existing dialog, the request has been sent from an AS in response to a previously sent request.

   - If not present, it indicates that the request is visiting the S-CSCF for the first time, and in this case the S-CSCF shall save the Request-URI from the request;

4) check whether the initial request matches the next unexecuted initial filter criteria in the priority order and apply the filter criteria on the SIP method as described in 3GPP TS 23.218 [5] subclause 6.5. If there is a match, then insert the AS URI to be contacted into the Route header as the topmost entry followed by its own URI populated as specified in the subclause 5.4.3.4;

NOTE 1: Depending on the result of the previous process, the S-CSCF may contact one or more AS(s) before processing the outgoing Request-URI.

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

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

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

8) if necessary perform the caller preferences to callee capabilities matching according to draft-ietf-sip-caller-preferences [62];

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

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

   b) forward the request based on the Request-URI and skip the following steps;

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

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

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

   b) determine, from the destination public user identity, the saved Contact URI where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2. If there is more than one contact address saved for the destination public user identity, the S-CSCF shall:

       - if the fork directive in the Request Disposition header was set to "no-fork", forward the request to the contact with the highest qvalue parameter. In case no qvalue parameters were provided, the S-CSCF shall decide locally how to forward the request; otherwise

- fork the request or perform sequential search based on the relative preference indicated by the qvalue parameter of the Contact header in the original REGISTER request, as described in RFC3261 [26]. In case no qvalue parameters were provided, then the S-CSCF shall forward the request as directed by the Request Disposition header as described in draft-ietf-sip-callerprefs-10 [56B]. If the Request-Disposition header is not present, the S-CSCF shall decide locally whether to fork or perform sequential search among the contact addresses;

    c) build a Request-URI with the contents of the saved Contact URI determined in the previous step; and

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

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

12) optionally, apply any privacy required by RFC 3325 [34] to the P-Asserted-Identity header and apply the same privacy mechanism to the P-Access-Network-Info header;

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].

13) in case of an initial request for a dialog, either:

    - if the request is routed to an AS which is part of the trust domain, the S-CSCF can decide whether to record-route or not. The decision is configured in the S-CSCF using any information in the received request that may otherwise be used for the initial filter criteria. If the request is record-routed the S-CSCF shall create a Record-Route header containing its own SIP URI; or

    - if the request is routed elsewhere, create a Record-Route header containing its own SIP URI; and

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

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

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

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

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

3) execute the procedure described in step 4, 5, 6, 7, 8, 9, 10, 12 and 13 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction).

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

When the S-CSCF receives a 1xx or 2xx response to the initial request for a dialog (whether the user is registered or not), it shall:

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

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

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

    4)   in case the response is sent towards the terminating user, the S-CSCF may remove the P-Access-Network-Info header based on local policy rules and the destination user (Request-URI).

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

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

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

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

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

    3)   create a Record-Route header containing its own SIP URI; and

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

When the S-CSCF receives a 1xx or 2xx response to the target refresh request for a dialog (whether the user is registered or not), the S-CSCF shall:

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

    2)   in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. In case the response is sent towards the terminating user, the S-CSCF may remove the header based on local policy rules and the destination user (Request-URI).

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

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

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

When the S-CSCF receives a response to a a subsequent request other than target refresh request for a dialog, in case the response is forwarded to an AS that is located within the trust domain, the S-CSCF shall retain the P-Access-Network-Info header; otherwise, the S-CSCF shall remove the P-Access-Network-Info header. In case the response is sent towards the terminating user, the S-CSCF may remove the header based on local policy rules and the destination user (Request-URI).

<div style="text-align:center; border:1px solid #000;">*** END OF MODIFICATION ***</div>