

**Source:** TSG CN WG 1  
**Title:** CRs to Rel-5 on Work Item IMS-CCR towards 24.229  
**Agenda item:** 8.1  
**Document for:** APPROVAL

---

**Introduction:**

This document contains 9 CRs on Rel-5 on Work Item "IMS-CCR", that have been agreed by TSG CN WG1, and are forwarded to TSG CN Plenary meeting #16 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Version Current	Version-New	Meeting-2nd-Level	Doc-2nd-Level
24.229	060	10	Rel-5	Restructuring of S-CSCF Registration Sections	F	5.0.0	5.1.0	N1-24	N1-021511
24.229	061	2	Rel-5	Determination of MOC / MTC at P-CSCF and S-CSCF	F	5.0.0	5.1.0	N1-SIP0204	N1-021060
24.229	062		Rel-5	Correction to the terminating procedures	F	5.0.0	5.1.0	N1-23	N1-020927
24.229	063		Rel-5	Loose Routing for Network Initiated Call Release Procedures	F	5.0.0	5.1.0	N1-23	N1-020940
24.229	064		Rel-5	Incorporation of previously agreed corrections to clause 5.2.5.2 (N1-020416)	F	5.0.0	5.1.0	N1-SIP0204	N1-021004
24.229	065		Rel-5	Clause 7.2 editorial corrections	D	5.0.0	5.1.0	N1-SIP0204	N1-021005
24.229	067	2	Rel-5	S-CSCF routing of MO calls	B	5.0.0	5.1.0	N1-SIP0204	N1-021097
24.229	068	1	Rel-5	I-CSCF routing of dialog requests	F	5.0.0	5.1.0	N1-SIP0204	N1-021078
24.229	069	2	Rel-5	Definition of the Tokenised-by parameter	F	5.0.0	5.1.0	N1-SIP0204	N1-021096

## CHANGE REQUEST

⌘ **24.229 CR 060** ⌘ rev **10** ⌘ Current version: **5.0.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Restructuring of S-CSCF Registration Sections		
<b>Source:</b>	⌘ Orange France, Ericsson, Vodafone, dynamicsoft, NEC Corporation, Lucent Technologies		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 17-May-2002
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ Rel-5
	<i>Use one of the following categories:</i> <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		<i>Use one of the following releases:</i> <b>2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>REL-4</b> (Release 4) <b>REL-5</b> (Release 5)

**Reason for change:** ⌘ The registration sections for S-CSCF do not clearly differentiate between the various cases for which a REGISTER request can be received (initial REGISTER, answer to authentication challenge, re-REGISTER). In addition, the S-CSCF informs the HSS that is serving a given user by passing to it its SIP URL. The Registration scenario needs modifying to align with the IETF Path and P-Service-Route headers.

Introduction of Subscription Locator Function Interrogation at S-CSCF: Subscription Locator Function has been introduced in stage 2 specification TS23.228 and in TS29.228 so that the HSS handling the subscription of a user can be found when there are several HSS in the Home network.  
 This needs to be reflected in TS24.229.  
 This CR covers S-CSCF case.  
 CR081 (Tdoc N1-021108) covers I-CSCF case

This CR adds support for barred and non barred public user identities downloaded from the HSS, in order to support UICCs that do not contain the ISIM application.

In 5.4.1.2.1, Cx procedure name needs to be aligned with 29.229.  
 There is ambiguity whether initial criteria is retrieved from initial registration and reregistration.

The XML-based solution for passing the charging-vector is updated with the P-header mechanism according to the internet-draft that has been submitted for a P-header version of charging-vector.

The CR adds text related to the introduction of the P-access-network-info header.

Version 10 of this CR incorporates to section 5.4.1.2.1 the changes due to CR 079.

**Summary of change:** ⌘ It is proposed to restructure the text for S-CSCF registration section as shown below.

Additionally,

- Update of 29.229 title in the Reference paragraph
- Addition due to SLF interrogation in step 4 of S-CSCF handling registration (§5.4.1.2.1)
- It is proposed to change the procedure name aligned with 29.229.
- It is also proposed to add the sentence stating that filter criteria is included in user profile and stored in the local data for re-registration or mobile origination call.
- The XML definitions are removed. Procedures are modified using the P-header fields instead of the XML elements for charging-vector.
- Behaviour relating to the P-access-network-info header is added

**Consequences if not approved:**

⌘ It will be unclear for the reader which procedures the S-CSCF needs to perform when receiving a REGISTER and the registration procedures will not align with IETF SIP.

Misalignment with stage 2 regarding SLF

There is not support for UICCs that do not contain the ISIM application.

It will be unclear for the reader how to get the initial Filter Criteria when initial registration and reregistration.

XML-based solution will be used to pass charging-vector instead of P-header.

**Clauses affected:**

⌘ 2, 5.4.1.2

**Other specs affected:**

⌘  Other core specifications ⌘   
 Test specifications  
 O&M Specifications

**Other comments:**

⌘ The procedures for P-CSCF and UE registration handling also need to be reworked. This CR is a first proposal to show how also the P-CSCF/UE rework should be done. If this CR is accepted, Siemens is willing to come up with further CRs on this subject.

Section 5.4.1.2.2 (abnormal cases) also needs some update, which should be in-line with the normal procedures section – if this CR is accepted, Siemens is willing to come up with an additional CR on this subject.

This CR also reflect the changes as agreed in document N1-020907 / CR 24.228 011, revision 1.

Revision 3 of this document was created in order to add text to sub-clause 5.4.2.1 in order to explain how is the protocol and port information conveyed to the HSS.

Revision 8 of this document was created to add text regarding SLF interrogation to find the correct HSS handling the user's subscription, to add the concept of barred and non-barred public user identities, to align with IETF Path and P-Service-Route headers, to reflect the changes as agreed in document N1-020907 / CR 24.228 011, revision 1.

**CHANGE #1**

---

## 2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

- [1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".
- [2] 3GPP TS 23.002: "Network architecture".
- [3] 3GPP TS 23.003: "Numbering, addressing and identification".
- [4] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".
- [5] 3GPP TS 23.218: "IP Multimedia (IM) Session Handling; IM call model".
- [6] 3GPP TS 23.221: "Architectural requirements".
- [7] 3GPP TS 23.228: "IP multimedia subsystem; Stage 2".
- [8] 3GPP TS 24.008: "Mobile radio interface layer 3 specification; Core Network protocols; Stage 3".
- [9] 3GPP TS 25.304: "UE Procedures in Idle Mode and Procedures for Cell Reselection in Connected Mode".
- [10] 3GPP TS 26.235: "Packet switched conversational multimedia applications; Default codecs".
- [11] 3GPP TS 29.208: "End to end Quality of Service (QoS) signalling flows".
- [12] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx Interface; Signalling flows and message contents".
- [12A] 3GPP TS 29.229: "Cx and Dx Interfaces based on the Diameter protocol, Protocol details".
- [13] 3GPP TS 33.102: "3G Security; Security architecture".
- [14] 3GPP TS 33.203: "Access security for IP based services".
- [15] 3GPP TS 44.018: "Mobile radio interface layer 3 specification, Radio Resource Control Protocol".
- [16] RFC 2806: "URLs for Telephone Calls".
- [17] RFC 2833 (May 2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".
- [18] RFC 2916: "E.164 number and DNS".
- [19] RFC 2976 (October 2000): "The SIP INFO method".
- [20] draft-ietf-sip-rfc2543bis-07 (January 2002): "SIP: Session Initiation Protocol".

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

- [21] draft-ietf-sip-100rel-05 (February 2002): "Reliability of provisional responses in SIP".

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

- [22] draft-sip-manyfolks-resource-03 (November 2001): "Integration of resource management and SIP".

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

- [23] draft-ietf-sip-events-02.txt (February 2002): "SIP-Specific Event Notification".

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

[24] draft-ietf-sip-callerprefs-05 (November 2001): "SIP caller preferences and callee capabilities".

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

[25] draft-ietf-sip-refer-02 (October 2001): "The REFER method".

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

[26] draft-ietf-sip-session-timer-08 (October 2001): "The SIP session timer".

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

[27] draft- sip-privacy-03 (November 2001): "SIP extensions for caller identity and privacy".

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

[28] draft- sip-state-02 (August 2001): "SIP extensions for supporting distributed call state".

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

[29] draft- sip-call-auth-03 (November 2001): "SIP extensions for media authorization".

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

[30] draft-ietf-mmusic-sdp-new-04 (November 2001): "SDP: Session Description Protocol".

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

[31] draft-mills-sip-access-network-info-01.txt (April 2002): "SIP Access Network Information header"

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

## CHANGE #2

### 5.4.1.2 Initial registration and user-initiated reregistration

#### 5.4.1.2.1 Initial registration

Upon receipt of a REGISTER request for a user that is not registered and for which also no authentication is currently ongoing (i.e. timer reg-await-auth is not running), 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) check the value of the Expires header. The S-CSCF shall only proceed with the following procedures if the Expires header is set to a value greater than zero;
- 4) 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 [12A], the S-CSCF shall select an authentication vector as described in 3GPP TS 33.203 [14]; 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 [12].

NOTE 1: 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 URL 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.

- 5) store the **icid parameter received in the P-Charging-Vector header;**6) **remove the p-access-network-info header and may act upon the contents accordingly.**
- 7) 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 7.2.3);
  - optionally the CK (Cipher Key) parameter for the P-CSCF in the ck field (see subclause 7.2.3);8) send the so generated 401 (Unauthorized) response towards the UE; and,
- 9) start timer reg-await-auth which guards the receipt of the next REGISTER request.

While timer reg-await-auth is running, Upon receipt of a REGISTER request, 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) stop timer reg-await-auth;
- 3) check whether the P-CSCF included the Integrity-protection field of the Authorization header set to yes, indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps if the integrity check parameter is included;
- 4) check whether an Authorization header is included, containing:
  - the private user identity of the user in the username field;
  - the algorithm which is AKAv1-MD5 in the algorithm field; **and**
  - the RES parameter needed for the authentication procedure in the response field.

The S-CSCF shall only proceed with the following steps in this paragraph if the RES parameter was included;

- 5) check whether the received RES parameter and the XRES parameter match. The XRES parameter was received from the HSS as part of the Authentication Vector. The S-CSCF shall only proceed with the following steps if RES and XRES are matching;
- 6) after performing the Cx **Server Assignment** procedure with the HSS, **as described in 3GPP TS 29.229 [12A],** store the following information **in the local data:**
  - the list of public user identities **associated to the user, including the own public user identity under registration and the implicitly registered due to the received REGISTER request; Each public user identity is identified as either barred or non-barred;** and,
  - the user profile of the user **including initial Filter Criteria;**
- 7) bind to each **non-barred** registered public user identity all registered contact information;

NOTE 2: There might be more than one contact information available for one public user identity.

**NOTE 3: The barred public user identities are not bound to the contact information.**

- 8) check whether a Path header was included in the REGISTER request and construct a list of preloaded Route headers from the list of entries in the Path header. The S-CSCF shall preserve the order of the preloaded Route headers and bind them to the contact information that was received in the REGISTER message;

NOTE 4: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.

- 9) determine the duration of the registration by checking the value of the Expires header in the received REGISTER request. The S-CSCF may adjust the duration of the registration due to local policy;
  - 10) store the **icid parameter received in the P-Charging-Vector header;**
  - 11) **remove the p-access-network-info header and may act upon the contents accordingly.**
  - 12) create a 200 (OK) response for the REGISTER request, including:
    - an expiration time in the Expires header, using one value provided within the S-CSCF, according to the local policy of the network, if this expiration time is shorter than the requested expiry time received from the UE; and,
    - the list of received Path headers;
    - a P-Associated-URI header containing the list of public user identities that the user is authorized to use. Such a collection of public user identities may or may not be implicitly registered by the network;
    - **a P-Service-Route header containing:**
      - **the SIP URL identifying the S-CSCF; and,**
      - **an indication that requests routed via the service route (i.e. from the P-CSCF to the S-CSCF) shall be treated as for the mobile originating case. This indication may e.g. be in a URI parameter, a character string in the user part or be a port number;**
      - **if network topology hiding is required a SIP URL identifying an I-CSCF(THIG) as the topmost entry;**
  - 13) send the so created 200 (OK) response to the UE;
  - 14) send a third-party REGISTER request, as described in subclause 5.4.1.7, to each Application Server that matches the Filter Criteria from the HSS for the REGISTER event; and,
- NOTE 5: If this registration is a reregistration, the Filter Criteria already exists in the local data.**
- 15) handle the user as registered for the duration indicated in the Expires header.

#### 5.4.1.2.2 User-initiated reregistration

Upon receipt of a REGISTER request for an already registered user, 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 from header of the REGISTER request;
- 2) check whether the P-CSCF included the Integrity-protection field of the Authorization header set to yes, indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps if the field is set to yes;
- 3) check if the user needs to be reauthenticated.

The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for registration requests received without integrity protection by the P-CSCF. The information that a REGISTER request was received integrity protected at the P-CSCF may be used as part of the decision to challenge the user.

If the user needs to be reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1, beginning with step 4). If the user does not need to be reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph;

- 4) check whether an Expires timer is included in the REGISTER request and its value. If the Expires header indicates a zero value, the S-CSCF shall perform the deregistration procedures as described in **subclause 5.4.1.4**. If the Expires header does not indicate zero, the S-CSCF shall proceed with the procedures as described for the second REGISTER in subclause 5.4.1.2, beginning with step 7); **and5) remove the p-access-network-info header and may act upon the contents accordingly.**

#### 5.4.1.2.3 Abnormal cases

In the case that the authentication response from the UE is incorrect the S-CSCF shall either:

- attempt a further authentication challenge; or
- deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the response from the UE is incorrect for three consecutive attempts then the S-CSCF shall deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the S-CSCF determines that no response will be received from the UE (e.g. it may be unreachable due to loss of radio coverage), the S-CSCF shall either:

- attempt a further authentication challenge; or
- deregister the user and terminate any ongoing sessions for all public user identities associated with the private user identity being authenticated, and release resources allocated to those sessions.

In the case that the response from the UE indicates that the authentication challenge was invalid with no RES or AUTS parameter in the subsequent REGISTER message, the S-CSCF shall:

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

In the case that the response from the UE indicates that the authentication challenge was invalid with the AUTS parameter in the subsequent REGISTER message, the S-CSCF shall:

- fetch new authentication vectors from the HSS, including AUTS and RAND in the request to indicate a resynchronisation; and
- on receipt of the new vectors send a 401 Unauthorized to initiate a further authentication attempt, using these new vectors.

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

- reject the REGISTER with a 423 Registration Too Brief, containing a Min-Expires header with the minimum registration time the S-CSCF will accept.

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

**CHANGE #3**

#### 5.4.3.2 Requests terminated at the served user

When the S-CSCF receives, destined for 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:

- remove its own URL from the topmost Route header;
- check if <original-dialog-id> XML element is present in the payload of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data



on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;

- check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous check the S-CSCF may contact one or more application server(s) before contacting an I-CSCF/P-CSCF respectively. In case of contacting one or more application server(s) the S-CSCF shall:
  - insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and
  - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.
- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;
- 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;
- determine, from the destination public user identity, the saved Contact URL where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2;
- build the Request-URI and Request header field values from the preloaded routes and saved Contact URL, as described in RFC 2543bis [20];
- insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;
- in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed;
- replace the Request-URI with the contents of the user Contact URL saved by the S-CSCF at registration time; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and
- forward the request based on the topmost Route header.

CR-Form-v5

## CHANGE REQUEST

⌘ **24.229 CR 061** ⌘ rev **2** ⌘ Current version: **5.0.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Determination of MOC / MTC at P-CSCF and S-CSCF		
<b>Source:</b>	⌘ Siemens AG		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 12.04.2002
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ Rel-5
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> of the following releases: <b>2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>REL-4</b> (Release 4) <b>REL-5</b> (Release 5)

<b>Reason for change:</b>	⌘ The procedures for P- and S-CSCF are described differently for MOC and MTC, although there is no description in 24.229 how the CSCF's determine whether a message is for the MO or the MO case.
<b>Summary of change:</b>	⌘ It is proposed that P-CSCF adds during registration an indication for MTC to its own entry in the Path header. When receiving a MTC message, the topmost Route header entry is a copy of this Path header entry. The same is proposed for the S-CSCF. Additional minor re-structuring and clarifications are made to the registration section for the S-CSCF (5.4.1.2).
<b>Consequences if not approved:</b>	⌘ It would stay an implementation option how a CSCF can determine MT/MO case.

<b>Clauses affected:</b>	⌘ 5.2.2, 5.2.6.2, 5.4.1.2, 5.4.3.1	
<b>Other specs affected:</b>	⌘ <input type="checkbox"/> Other core specifications ⌘ <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	
<b>Other comments:</b>	⌘ As the adoption of the IETF SIP replacements for the currently in 3GPP used Path header, these changes are written for the "old" Path-header. The related changes can be done in a revision, if 3GPP CN1 decides to adopt the two new headers (which is strongly recommended by the author). The registration sections for P-CSCF and especially S-CSCF need detailed re-work – the minor changes made in this contribution are only done in order to gain the MO/MT case determination functionality. <a href="#">Revision#2 was made in order to re-number sub-clauses and references.</a>	

## CHANGE #1

### 5.2.2 Registration

When the P-CSCF receives a REGISTER request from the UE that pertains to a given public user identity, the P-CSCF shall:

- 1)- insert a Path header in the request including. ~~The P-CSCF shall include in the Path header~~ an entry containing:
  - the SIP URL identifying the P-CSCF;
  - an indication that requests routed in this direction of the path (i.e. from the S-CSCF to the P-CSCF) shall be treated as for the mobile-terminating case. This indication may e.g. be in a Path header parameter, a character string in the user part or be a port number;
- 2)- insert a Require header and a Proxy-Require header both containing the option tag "path";
- 3)- if the REGISTER request was received with a valid integrity check, add information to the REGISTER request to indicate that the REGISTER request was received with a valid integrity check; and

**Editor's Note :** The exact mechanism for this is FFS.

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

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

- 1) remove its SIP URL from the list of Path headers, reverses the order of the list and save the resulting list of Path headers. This list shall be stored during the entire registration period of the respective public user identity. This list shall be used to preload the routing information into the initial requests originated by the UE. If this registration is a reregistration, the P-CSCF shall replace the already existing Path headers with the new list;
- 2) associate the Path header information with the registered public user identity;
- 3) remove the list of Path headers and "path" option-tags from the 200 OK response before forwarding the response to the UE.

When the P-CSCF receives a 401 Unauthorized response to a REGISTER request, the P-CSCF shall remove and store the CK and IK values contained in the 401 Unauthorized response. The 401 Unauthorized response shall be forwarded to the UE if and only if the CK and IK have been removed.

**Editor's Note:** The P-CSCF behaviour when 3xx or 4xx responses other than 401 Unauthorized are received is FFS.

**Editor's Note:** The text above assumes that public user identities are registered one by one. Public user identity might need to be changed to Service Profile in the case when public user identities can be implicitly registered.

**NOTE:** The P-CSCF will maintain two Route lists. The first Route list - created during the registration procedure - is used only to pre-load the routing information into the initial INVITE request that originated at the UE. This list is valid during the entire registration of the respective public user identity. The second Route list - constructed from the Record Route headers in the initial INVITE and associated response - is used during the duration of the call. Once the call is terminated, the second Route list is discarded.

When the P-CSCF receives a 420 Bad Extension response to the above REGISTER request, the P-CSCF shall check the value of the Unsupported header field. When the value of the Unsupported header field is path, the P-CSCF shall take OA&M actions to indicate an error, in addition to passing on the 420 response to the UE. In all other cases, the P-CSCF shall proxy the 420 Bad Extension response.

## CHANGE #2

### 5.2.6 General treatment for all dialogs and standalone transactions excluding the REGISTER method

#### 5.2.6.1 Introduction

The procedures of subclause 5.2.6 and its subclauses are general to all requests and responses, except those for the REGISTER method. Procedures in subsequent clauses to subclause 5.2.6 apply in addition to the procedures of subclause 5.2.6.

#### 5.2.6.2 Determination of mobile-originated or mobile-terminated case

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

- perform the procedures for the mobile-terminating case as described in subclause 5.2.6.4 if the request ~~facilitated~~ makes use of the information ~~topmost Route header entry contained the indication for mobile-~~terminating calls, which was added to the Path header entry of the P-CSCF during registration (see subclause 5.2.2) , e.g. the message is received at a certain port or the topmost Route header contains a specific user part or parameter;
- perform the procedures for the mobile-originating case as described in subclause 5.2.6.3 if this information is not ~~facilitated~~ used by the request ~~indication is not included in the topmost Route header entry.~~

#### 5.2.6.3~~2~~ Requests initiated by the UE

When the P-CSCF receives from the UE an initial request for a dialog, and a Path header list exists for the initiator of the request, the P-CSCF shall:

- remove any Route header from the request;
- select the list of Route headers that was created during the registration or reregistration of the respective public user identity utilizing the Path mechanism (see subclause 5.2.3);
- pre-load the list of Route headers to the request;
- create a Record-Route header containing its own SIP URL;
- create a new, globally unique value for the <icid> XML element and insert it into the message body (see subclause 7.6); and
- forward the request based on the topmost Route header.

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

- remove the list of Record-Route headers from the received response; and
- create a new list of stored Route headers, with the newly received list of Record-Route headers. The Contact header received in the response shall not be appended to the bottom of the stored list of Route headers.

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

- remove any list of Record-Route headers, even though not allowed, from the received response and forward it to the UE.

When the P-CSCF receives from the UE a refresh request for a dialog, the P-CSCF shall:

- remove any Route header from the request;
- select the list of Route headers that was created during the exchange of the initial request and its associated response;
- pre-load the list of Route headers to the request;
- create a Record-Route header containing its own SIP URL; and
- forward the request based on the topmost Route header.

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

- remove the list of Record-Route headers from the received response; and
- overwrite any existing list of stored Route headers, or create a new list of stored Route headers, with the newly received list of Record-Route headers. The Contact header received in the response shall not be appended to the bottom of the stored list of Route headers.

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

- remove any list of Record-Route headers, even though not allowed, from the received response and forward it to the UE.

When the P-CSCF receives from the UE the request for a standalone transaction, and a Path header list exists for the initiator of the request, the P-CSCF shall:

- remove any Route header from the request;
- select the list of Route headers that was created during the registration or reregistration of the respective public user identity utilizing the Path mechanism (see subclause 7.2.1);
- pre-load the list of Route headers to the request;
- create a new, globally unique value for the <icid> XML element and insert it into the message body (see subclause 7.6); and
- forward the request based on the topmost Route header.

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

- remove any list of Record-Route headers, even though not allowed, from the received response and forward it to the UE.

When the P-CSCF receives from the UE subsequent requests other than a refreshing request that pertains to an existing dialog, the P-CSCF shall:

- select the list of Route headers that was created during the exchange of the initial request and associated response for this call;
- pre-load the list of Route headers to the request; and
- forward the request based on the topmost Route header.

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

- remove any list of Record-Route headers, valid or not, from the received response and forward it to the UE.

When the P-CSCF receives from the UE an initial request for a dialog, a refresh request for a dialog, or the request of a standalone transaction, and a Path header list does not exist for the initiator of the request, the P-CSCF shall:

- send a 403 Forbidden response back to the UE containing a warning header.

Editor's Note: how to find out whether the user has a valid registration in the P-CSCF is FFS.

Editor's Note: The correct value for the warning code is yet to be assigned by IANA.

When the P-CSCF receives from the UE the request for an unknown method, and a Path header list exists for the initiator of the request, the P-CSCF shall:

- select the list of Route headers that was created during the registration or reregistration of the respective public user identity utilizing the Path mechanism (see subclause 7.2.1);
- pre-load the list of Route headers to the request, and
- forward the request based on the topmost Route header.

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

- remove any list of Record-Route headers, even though invalid, from the received response and forward it to the UE.

When the P-CSCF receives any request or response from the UE, the P-CSCF shall:

- remove the <charging-vector> XML element (see subclause 7.6), if present, from the message body of the received request or response.

### 5.2.6.43 Requests terminated by the UE

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

- remove its own SIP URL from the topmost Route header;
- remove the list of Record-Route headers, and shall convert it into a list of Route headers. The Contact header shall not be appended to the bottom of the list of Route headers. The P-CSCF shall save this list of Route headers and append this list to all UE originated requests for this dialog;
- add itself on the top of the removed list of Record-Route headers and save the list. The list will be appended to UE originated response to the SUBSCRIBE request;
- remove and store the list of received Via headers from the received request and shall place its own address in the Via header with locally unique token to identify the saved values as a branch parameter . The P-CSCF shall append the list of Via headers to the UE originated response for this request; and
- remove and store the <icid> XML element from the message body (see subclause 7.6).

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

- append the saved list of Record-Route headers to the response; and,
- append the saved list of Via headers to the response.

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

- append the saved list of Via headers to the response.

When the P-CSCF receives, destined for the UE, a subsequent request for a dialog that is not a refresh request, or a request for a stand-alone transaction, prior to forwarding the request, the P-CSCF shall:

- remove and store the list of received Via headers from the received request and shall place its own address in the Via header with locally unique token to identify the saved values as a branch parameter . The P-CSCF shall append this list of Via headers to the UE originated response for this transaction; and
- remove and store the <icid> XML element from the message body (see subclause 7.6).

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

- append the saved list of Via headers to the response.

When the P-CSCF sends any request or response to the UE, the P-CSCF shall:

- remove the <charging-vector> XML element (see subclause 7.6) from the message body of the request or response.

## **CHANGE #3**

### 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 refresh request or a stand-alone transaction, the S-CSCF shall:

- perform the procedures for the mobile-terminating case as described in subclause 5.4.3.3 if this indication information is not facilitated used by the request is not included in the user part of the Request URI.
- perform the procedures for the mobile-originating case as described in subclause 5.4.3.2 if the request facilitated makes use of the information topmost Route header entry contained the indication for mobile-originating calls, which was added to the Path 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,

#### 5.4.3.2~~1~~ 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:

- remove its own SIP URL from the topmost Route header;
- if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [16]) to a globally routable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [18]. 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 an appropriate SIP response shall be sent to the originator;
- check if <original-dialog-id> XML element is present in the payload of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;
- check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous check, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:
  - insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and
  - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the

message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.43 for further information on the original dialog identifier.

- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;
- determine the destination address (e.g. DNS access) using the URL placed in the topmost Route header if present, otherwise based on the Request-URI; and
- in case of an initial request for a dialog the S-CSCF shall create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed.

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and
- route the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and
- route the request based on the topmost Route header.

### 5.4.3.32 Requests terminated at the served user

When the S-CSCF receives, destined for 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:

- remove its own URL from the topmost Route header;
- check if <original-dialog-id> XML element is present in the payload of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;
- check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous check the S-CSCF may contact one or more application server(s) before contacting an I-CSCF/P-CSCF respectively. In case of contacting one or more application server(s) the S-CSCF shall:
  - insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and
  - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.43 for further information on the original dialog identifier.
- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;



- 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 5.4.1.2.1;
- determine, from the destination public user identity, the saved Contact URL where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2.1;
- build the Request-URI and Request header field values from the preloaded routes and saved Contact URL, as described in RFC 2543bis [20];
- insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;
- in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed;
- replace the Request-URI with the contents of the user Contact URL saved by the S-CSCF at registration time; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and
- forward the request based on the topmost Route header.

#### 5.4.3.43 Original dialog identifier

The original dialog identifier is coded as the <original-dialog-id> XML element within the SIP message body as described in subclause 7.6.

For the messages including the <original-dialog-ID> XML element, set the value of the Content-Type header to include the MIME type specified in subclause 7.6, which may be one part of a multipart message body.

#### 5.4.3.54 Abnormal cases

The S-CSCF shall, when contacting application servers based on the initial filter criteria, expect either a final response from the application server as the session terminates there, or the initial request message, that may be modified. In either case the message should be identified (using <original-dialog-id> XML element) as belonging to the original request forwarded by the S-CSCF.

If the S-CSCF receives a message including an <original-dialog-id> XML element that does not match any that it has forwarded to the application server it shall:

- respond to the application server with 481 Call Leg/Transaction Does Not Exist.

**CHANGE #3**

7.2.2.3      Operation

The operation of this header is described in subclause 5.4.3.~~32~~.

CR-Form-v5

## CHANGE REQUEST

⌘ **24.229 CR 062** ⌘ rev **-** ⌘ Current version: **5.0.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Correction to the terminating procedures		
<b>Source:</b>	⌘ Ericsson		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 11-Apr-02
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ REL-5
	<i>Use one of the following categories:</i> <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900.	<i>Use one of the following releases:</i> <b>2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>REL-4</b> (Release 4) <b>REL-5</b> (Release 5)	

<b>Reason for change:</b>	⌘ The current text that describes how the S-CSCF builds the Route header and the Request-URI in terminating cases is not clear.
<b>Summary of change:</b>	⌘ Clarification on the procedures at the S-CSCF with respect Route headers and Request-URIs.
<b>Consequences if not approved:</b>	⌘ Misleading text leading to erroneous implementations.

<b>Clauses affected:</b>	⌘ 5.4.3.2		
<b>Other specs affected:</b>	<input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘	
<b>Other comments:</b>	⌘		

### How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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 terminated at the served user

When the S-CSCF receives, destined for 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:

- remove its own URL from the topmost Route header;
- check if <original-dialog-id> XML element is present in the payload of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;
- check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.5. Depending on the result of the previous check the S-CSCF may contact one or more application server(s) before contacting an I-CSCF/P-CSCF respectively. In case of contacting one or more application server(s) the S-CSCF shall:
  - insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and
  - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.
- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;
- 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 5.4.1.2.1;
- build the Route header field with the values determined in the previous step;
- determine, from the destination public user identity, the saved Contact URL where the user is reachable saved at registration or reregistration, as described in subclause 5.4.1.2.1;
- build a Request-URI with the contents of the saved Contact URL determined in the previous step;
- ~~- build the Request-URI and Request header field values from the preloaded routes and saved Contact URL, as described in RFC 2543bis [20];~~
- insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;
- in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and
- ~~- replace the Request-URI with the contents of the user Contact URL saved by the S-CSCF at registration time; and~~
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and
- forward the request based on the topmost Route header.

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

- remove its own URL from the topmost Route header; and
- forward the request based on the topmost Route header.

CR-Form-v5

## CHANGE REQUEST

⌘ **24.229** CR **063** ⌘ rev - ⌘ Current version: **5.0.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Loose Routing for Network Initiated Call Release Procedures		
<b>Source:</b>	⌘ Siemens AG, Nokia		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 02.04.2002
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ Rel-5
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> 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)

<b>Reason for change:</b>	⌘ During the last CN1 meeting the procedures for loose routing and network initiated call release were introduced in parallel. This CR applies loose routing to the network initiated call release procedures.
<b>Summary of change:</b>	⌘ It is proposed to apply loose routing also for network initiated call release procedures.
<b>Consequences if not approved:</b>	⌘ Network initiated call release will be not be in-line with the IETF SIP loose routing procedures as well as the rest of 24.229 specification (where loose routing was already adopted)

<b>Clauses affected:</b>	⌘ 5.2.8.1.2, 5.4.5.1.2		
<b>Other specs affected:</b>	<input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘	
<b>Other comments:</b>	⌘		

### 5.2.8.1.2 Release of an existing session

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

- 1) ~~If~~ if the P-CSCF serves the calling user of a session it shall generate a BYE message based on the information saved for the related dialog, including:
  - a Request-URI, set to the stored Contact header provided by the called user ~~set to the topmost entry of the stored routing information to the contact information of the called user, as received in the 200 OK response for the initial INVITE request towards the called user;~~

Contributors Note: The above change is in-line with the changes proposed in N1-020799 by Lucent/Milo, which was pre-agreed.

- a To header, set to the To header value as received in the 200 OK response for the initial INVITE request;
  - a From header, set to the From header value as received in the initial INVITE request;
  - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
  - a CSeq header, set to the CSeq value that was stored for the direction from the calling to the called user, incremented by one;
  - a Route header, set to the routing information towards the called user as stored for the dialog; ~~exclusively the topmost entry (which appears in the Request URI);~~
  - further headers, based on local policy or the requested session release reason.
- 2) ~~if~~ if the P-CSCF serves the called user of a session it shall generate a BYE message based on the information saved for the related dialog, including:
    - a Request-URI, set to ~~the topmost entry of the stored routing information towards the calling user~~ the stored Contact header provided by the calling user ~~the contact information of the calling user, as received in the initial INVITE request;~~
    - a To header, set to the From header value as received in the initial INVITE request;
    - a From header, set to the To header value as received in the 200 OK response for the initial INVITE request;
    - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
    - a CSeq header, set to the CSeq value that was stored for the direction from the called to the calling user, incremented by one – if no CSeq value was stored for that session it shall generate and apply a random number within the valid range for CSeqs;
    - a Route header, set to the routing information towards the calling user as stored for the dialog; ~~exclusively the topmost entry (which appears in the Request URI);~~
    - further headers, based on local policy or the requested session release reason.
  - 3) ~~Afterwards the P-CSCF shall~~ send the so generated BYE message towards the indicated user.
  - 4) upon receipt of the 2xx responses for the BYE request, ~~the P-CSCF shall~~ delete all information related to the dialog and the related multimedia session.

### 5.4.5.1.2 Release of an existing session

Upon receipt of a network internal indication to release an existing multimedia session, the S-CSCF shall:

- 1) generate a first BYE message for the called user based on the information saved for the related dialog, including:
  - a Request-URI, set to the [set to the stored Contact header provided by the called user](#)~~topmost entry of the stored routeing information towards contact information of the called user, as received in the 200 OK response for the initial INVITE request;~~
  - a To header, set to the To header value as received in the 200 OK response for the initial INVITE request;
  - a From header, set to the From header value as received in the initial INVITE request;
  - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
  - a CSeq header, set to the CSeq value that was stored for the direction from the calling to the called user, incremented by one;
  - a Route header, set to the routeing information towards the called user as stored for the dialog;  
~~exclusively the topmost entry (which appears in the Request URI);~~
  - further headers, based on local policy or the requested session release reason.
- 2) generate a second BYE message for the calling user based on the information saved for the related dialog, including:
  - a Request-URI, set to the [stored Contact header provided by the](#) ~~topmost entry of the stored routeing information towards contact information of the~~ calling user, ~~as received in the initial INVITE request;~~
  - a To header, set to the From header value as received in the initial INVITE request;
  - a From header, set to the To header value as received in the 200 OK response for the initial INVITE request;
  - a Call-ID header, set to the Call-Id header value as received in the initial INVITE request;
  - a CSeq header, set to the CSeq value that was stored for the direction from the called to the calling user, incremented by one – if no CSeq value was stored for that session it shall generate and apply a random number within the valid range for CSeqs;
  - a Route header, set to the routeing information towards the calling user as stored for the dialog;  
~~exclusively the topmost entry (which appears in the Request URI);~~
  - further headers, based on local policy or the requested session release reason.
- 3) ~~if the S-CSCF serves the calling user, it shall:~~
  - ~~treat the first BYE message as if received directly from the calling user, i.e. send it to internal service control and based on the outcome further on towards the called user;~~
- ~~4) if the S-CSCF serves the calling user, send the second BYE message directly to the calling user;~~
- ~~5) if the S-CSCF serves the called user it shall:~~
  - send the first BYE message directly to the called user;
- 6) ~~if the S-CSCF serves the called user, —~~ treat the second BYE message as if received directly from the called user, i.e. shall send it to internal service control and based on the outcome further on towards the called user.

Upon receipt of the 2xx responses for both BYE requests, the S-CSCF shall release all information related to the dialog and the related multimedia session.



CR-Form-v5

## CHANGE REQUEST

⌘ **24.229 CR 064** ⌘ rev **-** ⌘ Current version: **5.0.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Incorporation of previously agreed corrections to clause 5.2.5.2 (N1-020416)		
<b>Source:</b>	⌘ Lucent Technologies (previously Siemens, Nokia)		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 18/04/02
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ Rel-5
	Use <u>one</u> of the following categories:		Use <u>one</u> of the following releases:
	<b>F</b> (correction)		<b>2</b> (GSM Phase 2)
	<b>A</b> (corresponds to a correction in an earlier release)		<b>R96</b> (Release 1996)
	<b>B</b> (addition of feature),		<b>R97</b> (Release 1997)
	<b>C</b> (functional modification of feature)		<b>R98</b> (Release 1998)
	<b>D</b> (editorial modification)		<b>R99</b> (Release 1999)
	Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		<b>REL-4</b> (Release 4)
			<b>REL-5</b> (Release 5)

<b>Reason for change:</b>	⌘ A previously agreed change was not implemented by the editor prior to TSG CN agreement, and placing under change control.
<b>Summary of change:</b>	⌘ New text is proposed for 5.2.5.2 which removes conflicting text, resulting in a single text in accordance with existing agreements. No technical change is proposed. The proposed text is identical to that in the original N1-020416 with some very minor punctuation changes only. There appear to be not related changes that need to be taken into account since the original unimplemented document was agreed.
<b>Consequences if not approved:</b>	⌘ An editor's note will remain in the text and the conflicting text will continue to exist, providing for misinterpretation of the requirements.

<b>Clauses affected:</b>	⌘ 5.2.5.2		
<b>Other specs affected:</b>	⌘ <input type="checkbox"/> Other core specifications	⌘	
	<input type="checkbox"/> Test specifications		
	<input type="checkbox"/> O&M Specifications		
<b>Other comments:</b>	⌘ The original justification for the change was the following: " This contribution proposes to resolve the conflict caused by N1-011984 and N1-011988 in the de-registration section in 24.229."  Note that the change provided for in CR045R0 that relates to this clause is not longer applicable, as the affected text is deleted, and the new text does not contain the same error.		

### How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.htm). Below is a brief summary:

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

- 2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under <ftp://ftp.3gpp.org/specs/> For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
- 3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

## 5.2.5.2 Network-initiated deregistration

### If the P-CSCF:

- has subscribed for the registration-state event package providing registration state information of a certain public identity and public user identities implicitly registered with it; and,
- an incoming NOTIFY request arrives on the dialog which was generated during subscription (as described in subclause 5.2.3) containing the registration state value "closed", i.e. deregistered, for one or more public user identities;

the P-CSCF shall release all stored information for these public user identities which are indicated with registration state "closed".

~~If the P-CSCF has subscribed for the event providing registration state information of a certain public user identity and an incoming NOTIFY request addressed to P-CSCF arrives containing information about network-initiated deregistration, then the P-CSCF shall remove the deregistered public user identity from the registered public user identities list and all related stored information.~~

~~Editor's note: The above text came from N1-011984, the text below from N1-011988. The two texts are attempting to specify the same thing. This conflict needs to be resolved in a future contribution.~~

~~Upon receipt of a NOTIFY message on the dialog which was generated during subscription to the registration state event package as described in subclause 5.2.3, which contains the registration state value "closed", i.e. deregistered, for one or more public user identities that were previously stored as registered, the P-CSCF shall release all stored information for that public user identity of that user.~~

~~If all public user identities that have been bound to one contact information are marked as deregistered, the P-CSCF shall release all resources for that specific user, i.e. the user then is treated as deregistered from the IM-CN subsystem.~~

CR-Form-v5

## CHANGE REQUEST

⌘ **24.229 CR 065** ⌘ rev **-** ⌘ Current version: **5.0.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ Clause 7.2 editorial corrections		
<b>Source:</b>	⌘ Lucent Technologies		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 18/04/02
<b>Category:</b>	⌘ <b>D</b>	<b>Release:</b>	⌘ Rel-5
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> 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)

<b>Reason for change:</b>	⌘ Compliance with drafting rules.		
<b>Summary of change:</b>	⌘ Inclusion of table number and reference in the text. Provision of references in correct format.		
<b>Consequences if not approved:</b>	⌘ None.		

<b>Clauses affected:</b>	⌘ 7		
<b>Other specs affected:</b>	<input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘	
<b>Other comments:</b>	⌘		

### How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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.

---

## 7 Extensions within the present document

### 7.1 SIP methods defined within the present document

There are no SIP methods defined within the present document over and above those defined in the referenced IETF specifications.

### 7.2 SIP headers defined within the present document

#### 7.2.1 Path header

##### 7.2.1.1 Introduction

Path header is a mechanism whereby a P-CSCF, I-CSCFs, and S-CSCF can request to be on a signalling path for the initial INVITE exchanged between the UE and the S-CSCF. The path-establishment procedure is originated by the P-CSCF during the registration process. The procedure is performed during the initial registration of each public user identity and all subsequent reregistrations. The list of Path headers obtained by a reregistration overwrites the existing list of Path headers at the S-CSCF. Each reregistration of the same public user identity may result in new list of Path headers. The P-CSCF uses the list of Path headers to construct a list of Route headers. When initiating a call pertaining to a given public user identity, the list of Route headers will be pre-loaded into the initial INVITE request.. If a CSCF wants to receive subsequent requests, it will insert its own name to the Record Route header of the initial INVITE request. Once on the route, a CSCF remains on the route for the duration of the call. The path learned while reregistering during an active call does not affect the existing call, since the routing path for the respective call has already been established. The list of Path headers is not forwarded to the UE.

##### 7.2.1.2 Syntax

The Path header field has the syntax described in table 7.1.

**Table 7.1: Syntax of path header**

```
Path = "Path" ":" l#(name-addr *(";"rr-param))
rr-param = generic-param
```

##### 7.2.1.3 Operation

The operation of this header is described in clause 5.

### 7.2.2 P-Called-Party-ID header

#### 7.2.2.1 Introduction

The P-Called-Party-ID header is the mechanism whereby the terminating UE learns the dialled public user identity that triggered the current session initiation.

The S-CSCF inserts the header in all terminating INVITE and reINVITE requests. The header is not used in any other request or response.

### 7.2.2.2 Syntax

The P-Called-Party-ID header field has the syntax described in table 7.2.

**Table 7.2: Syntax of P-Called-Party-ID header**

<pre>P-Called-Party-ID = "P-Called-Party-ID" HCOLON 1#                     (name-addr *( SEMI p-cdpid-param))  p-cdpid-param = generic-param</pre>
--

Table 7.3 is an extension of tables 2 and 3 in RFC 2543bis [20] and table in subclause 7.5 in the SIP-specific event notification [23].

**Table 7.3: P-Called-Party-ID header**

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG	PRA	SUB	NOT
P-Called-Party-ID	R	am	-	-	-	o	-	-	-	-	-

### 7.2.2.3 Operation

The operation of this header is described in subclause 5.4.3.2.

## 7.3 Option-tags defined within the present document

### 7.3.1 "path" option-tag

A new option-tag "path" is added to the list of option-tags allowed for both Require and Proxy-Require headers.

The operation of this option tag is described in clause 5.

## 7.4 Status-codes defined within the present document

There are no status-codes defined within the present document over and above those defined in the referenced IETF specifications.

## 7.5 Session description types defined within the present document

There are no session description types defined within the present document over and above those defined in the referenced IETF specifications.

## 7.6 3GPP IM CN subsystem XML body, version 1

### 7.6.1 General

This subclause describes the Document Type Definition that is applicable for the 3GPP IM CN Subsystem XML body.

Any SIP User Agent or proxy may insert or remove the 3GPP IM CN subsystem XML body or parts of it, as required, in any SIP message. The <icid> XML element is an exception to this rule; it may only be removed by the P-CSCF. The 3GPP IM CN subsystem XML body shall not be forwarded outside a 3GPP network.

The associated MIME type with the 3GPP IMX XML body is "application/3gpp-ims+xml".

## 7.6.2 Document Type Definition

[The Document Type Definition, according to XML syntax definitions, is defined in Table 7.4.](#)

**[Table 7.4: 3GPP IM CN subsystem XML body, version 1 DTD](#)**

```
<?xml version="1.0" ?>
<!-- Draft DTD for the 3GPP IMS XML body. -->

<!DOCTYPE ims-3gpp [
  <!-- ims-3gpp element: root element -->

  <!ELEMENT ims-3gpp (vnid?, cell-id?,
    original-dialog-id?, destination-public-user-id?,
    access?, charging-vector?, service-info?)>
  <ATTLIST ims-3gpp version CDATA #REQUIRED>

  <!-- vnid element: Visited network identity -->
  <!ELEMENT vnid          (#PCDATA)>

  <!-- cell-id element: The Cell-Global-ID -->
  <!ELEMENT cell-id      (mcc, mnc, lac, ci)>
  <!ELEMENT mcc          (#PCDATA)>
  <!ELEMENT mnc          (#PCDATA)>
  <!ELEMENT lac          (#PCDATA)>
  <!ELEMENT ci           (#PCDATA)>
  <ATTLIST cell-id rat (utran | geran) #REQUIRED>

  <!-- original-dialog-id: original dialog ID -->
  <!ELEMENT original-dialog-id (od-from, od-to, od-call-id)>
  <!ELEMENT od-from        (#PCDATA)>
  <!ELEMENT od-to          (#PCDATA)>
  <!ELEMENT od-call-id     (#PCDATA)>

  <!-- public-user-id: public user ID -->
  <!ELEMENT destination-public-user-id (#PCDATA)>

  <!-- access: the type of access network →
  <!ELEMENT access        (access-type, technology?)>
  <!ELEMENT access-type   (gprs | wlan | fixed | (#PCDATA))>
  <!ELEMENT technology    (utran| geran | 802.11a |
    802.11b | sat | adsl | (#PCDATA))>

  <!-- charging-vector element: Charging Vector -->
  <!ELEMENT charging-vector (icid, gprs-charging-id?)>

  <!-- icid element: IMS charging identifier -->
  <!ELEMENT icid          (#PCDATA)>
  <!-- gprs-charging-id element: GPRS charging identifiers -->
  <!ELEMENT gprs-charging-id (ggsn, pdp-info+)>
  <!ELEMENT ggsn           (#PCDATA)>
  <!ELEMENT pdp-info       (pdp-index, pdp-id)>
  <!ELEMENT pdp-index      (#PCDATA)>
  <!ELEMENT pdp-id         (#PCDATA)>

  <!-- service-info element: The transparent data received from HSS for AS -->
  <!ELEMENT service-info  (#CDATA)>

  <!-- alternative-service: alternative-service used in emergency sessions -->
  <!ELEMENT alternative-service (type, reason)>
  <!ELEMENT type           (emergency)>
  <!ELEMENT reason         (#PCDATA)>

]>
```

## 7.6.3 DTD description

This section describes the elements of the 3GPP IMS Document Type Definition [as defined in Table 7.4.](#)

- <ims-3gpp>**: This is the root element of the 3GPP IMS XML body. It shall always be present. The version described in the present document is 1.
- <vnid>**: Visited network identifier. Optional element that describes the P-CSCF network name. The vnid value is a string of characters that identifies the P-CSCF network at the user's network home.
- <cell-id>**: This element describes the identity of the cell that is serving the user.
- The **<cell-id>** element contains the **<ran>** attribute that identifies the coding of the cell-id, according to whether the cell-id was received from the GERAN or UTRAN.
- The **<cell-id>** element comprises four children elements: **<mcc>**, **<mnc>**, **<lac>** and **<ci>**. They represent, respectively, the Mobile Country Code, Mobile Network Code, Location Area Code and Cell Identity, as described in [3].
- <original-dialog-id>**: The original dialog, as received by the S-CSCF. This element helps the S-CSCF to correlate dialogues when the Application Server is behaving as a B2BUA, and therefore, modifies then dialogue.
- The **<original-dialog-id>** element comprises three children elements: **<od-from>**, **<od-to>**, **<od-call-id>**. Their values contain, respectively, a copy of the From, To and Call-ID header values as received in the SIP message at the S-CSCF.
- <destination-public-user-id>**: The destination public-user-id URL of the current session.
- <access>**: The access element, if present, identifies the access that the UE is utilized to connect to the network. The element contains two children elements: **<ant>** and **<technology>**.
- The **<access-type>** child element describes the access type. The predefined values are:
- gprs: the user is accessing the network through a GRPS access;
  - wlan: the user is accessing the network through a wireless local area network;
  - fixed: the user is accessing the network through a fixed access.
- The **<technology>** child element, if present, describes the access technology. The pre-defined values are:
- utran: UTRAN, as defined in [3GPP TS 23.003](#) [3];
  - geran: GERAN, as defined in [3GPP TS 23.003](#) [3];
  - 802.11a: wireless local area network according to the 802.11a technology;
  - 802.11b: wireless local area network according to the 802.11b technology;
  - sat: satellite access;
  - adsl: asymmetric digital subscriber line.
- <charging-vector>**: the charging-vector element, if present, identifies charging correlation information. The element contains two children elements: **<icid>** and **<gprs-charging-id>**.
- The **<icid>** child element contains an IMS charging identifier that is globally unique and is associated with the end-to-end session.
- The **<gprs-charging-id>** child element, if present, contains GPRS charging identifiers comprised of the following: **<ggsn>** and **<pdp-info>**:
- **<ggsn>**: identifier of the GGSN;
  - **<pdp-info>**: one or more instances of information for a PDP context, which is comprised of two children elements: **<pdp-index>** and **<pdp-id>**:
    - **<pdp-index>**: relative index of PDP context as it correlates to a media stream in the SDP;



- <pdp-id>: unique identifier of the PDP context from the GGSN.

<service-info>: the transparent element received from the HSS for a particular Application Server are placed within this optional element.

<alternative-service>: in the present document, the alternative service is used as a response for an attempt to establish an emergency session within the IM CN subsystem. The element describes an alternative service where the call should success. The alternative service is described by the type of service information. A possible reason cause why an alternative service is suggested may be included.

The <alternative-service> element contains a <type> element that indicates the type of alternative service. In the present document, the <type> element contains only the value "emergency".

The <reason> element contains an explanatory text with the reason why the session setup has been redirected. A UE may use this information to give an indication to the user.

## CHANGE REQUEST

⌘ **24.229 CR 067** ⌘ rev **2** ⌘ Current version: **5.0.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ S-CSCF routing of MO calls		
<b>Source:</b>	⌘ Lucent Technologies, Siemens		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 2002-04-24
<b>Category:</b>	⌘ <b>B</b> Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .	<b>Release:</b>	⌘ <b>REL-5</b> Use <u>one</u> of the following releases: <b>2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>REL-4</b> (Release 4) <b>REL-5</b> (Release 5)

<b>Reason for change:</b>	⌘ Currently the document 24.229 does not specify how does the S-CSCF route the MO initial requests. The proposed text clarifies the routing procedure in the S-CSCF
<b>Summary of change:</b>	⌘ The S-CSCF handling session origination performs an annalysis of the destination SIP URL and determines whether pertains to a subscriber of the same network operator or a different operator. Subsequently it forwards the request accordingly.
<b>Consequences if not approved:</b>	⌘ It may result in inconsistent routing of initial requests in the IMS.

<b>Clauses affected:</b>	⌘ 5.4.3.2
<b>Other specs affected:</b>	⌘ <input type="checkbox"/> Other core specifications ⌘ <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications
<b>Other comments:</b>	⌘ This CR assumes that the CRs from the CN1#23 that are currently incorporated into the document 24.229 5.0.0 CN1#23 are accepted. This CR only adds some new text, and it does not modify any text in document 24.229 5.0.0 CN1#23. Revision 1 incorporates the changes to the original subclause 5.3.2.1 that was agreed during the meeting.

### How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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.

### 5.4.3.1 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:

- remove its own SIP URL from the topmost Route header;
  - if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [16]) to a globally routable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [18]. 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 an appropriate SIP response shall be sent to the originator;
  - check if <original-dialog-id> XML element is present in the payload of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;
  - check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous check, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:
    - insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and
    - initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the <original-dialog-id> XML element in the message body with the original To, From and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.
  - store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;
  - ~~—~~ determine the destination address (e.g. DNS access) using the URL placed in the topmost Route header if present, otherwise based on the Request-URI; ~~and~~
  - if network hiding is needed due to local policy, put the address of the I-CSCF(THIG) to the topmost route header; ~~and~~
- route the request based on SIP routing procedures;
- in case of an initial request for a dialog the S-CSCF shall create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; ~~and~~;
- route the request based on SIP routing procedures;

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

- remove its own URL from the topmost Route header;
- create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed; and
- route the request based on the topmost Route header.

~~Error! No text of specified style in document. Error! No text of specified style in document. Fehler! Kein Text mit angegebener Formatvorlage im Dokument.~~

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

- remove its own URL from the topmost Route header; and
- route the request based on the topmost Route header.

CR-Form-v5

## CHANGE REQUEST

⌘ **24.229 CR 068** ⌘ rev **1** ⌘ Current version: **5.0.0** ⌘

For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ I-CSCF routing of dialog requests		
<b>Source:</b>	⌘ Lucent, Siemens		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 2002-04-24
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ REL-5
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP TR 21.900.		Use <u>one</u> 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)

<b>Reason for change:</b>	⌘ Currently the document 24.229 does not addresses the routing of requests by I-CSCF <u>every detail</u> .
<b>Summary of change:</b>	⌘ By examining the Route list and knowing the source of the request, the I-CSCF invokes hiding and routes the request to the proper next hop.
<b>Consequences if not approved:</b>	⌘ Incomplete routing procedure

<b>Clauses affected:</b>	⌘ 5.3.2.1		
<b>Other specs affected:</b>	⌘ <input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘	
<b>Other comments:</b>	⌘ This CR assumes that the CRs from CN1#23 that are currently incorporated into the document 24.229 5.0.0 CN1#23 are accepted. This CR only adds some new text, and it does not modify any text in the document 24.229 5.0.0 CN1#23. Revision 1 incorporates the changes to the original subclause 5.3.2.1 that was agreed during the meeting.		

### How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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.

### 5.3.2.1 Normal procedures

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

When the I-CSCF receives an initial request, that either does not contain~~ing~~ a Route header or contains a single Route header pointing to itself, the I-CSCF shall start the user location query procedure to the HSS as specified in 3GPP TS 29.228 [12] for the called user, indicated in the Request-URI.

Upon successful user location query, the I-CSCF shall:

- 1) if present, remove its own SIP URL from the topmost Route header;
- 2) insert the URL received from the HSS as the topmost Route header;
- 3) store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body. If no <icid> XML element was found, then create a new, globally unique value for the <icid> XML element and insert it into the message body;
- 4) apply the procedures as described in subclause 5.3.3 if topology hiding is required; and
- 5) forward the request based on the topmost Route header.

When the I-CSCF receives an initial request containing more than one~~a~~ Route header, the I-CSCF shall:

- remove its own SIP URL from the topmost Route header;
- apply the procedures as described in subclause 5.3.3; and
- forward the request based on the topmost Route header if present, or based on the Request-URI, in case no topmost Route header is available.

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



CR-Form-v5

## CHANGE REQUEST

⌘ **24.229 CR 069** ⌘ rev **24** ⌘ Current version: **5.0.0** ⌘

For [HELP](#) on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.

**Proposed change affects:** ⌘ (U)SIM  ME/UE  Radio Access Network  Core Network

<b>Title:</b>	⌘ <del>Tokenised</del> Tokenized-by header definition		
<b>Source:</b>	⌘ Nokia		
<b>Work item code:</b>	⌘ IMS-CCR	<b>Date:</b>	⌘ 20-04-2002
<b>Category:</b>	⌘ <b>F</b>	<b>Release:</b>	⌘ REL-5
	<i>Use one of the following categories:</i> <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		<i>Use one of the following releases:</i> <b>2</b> (GSM Phase 2) <b>R96</b> (Release 1996) <b>R97</b> (Release 1997) <b>R98</b> (Release 1998) <b>R99</b> (Release 1999) <b>REL-4</b> (Release 4) <b>REL-5</b> (Release 5)

<b>Reason for change:</b>	⌘ There is no definition yet of this parameter. This CR describes the operation and BNF format of the parameter
<b>Summary of change:</b>	⌘ No change to the current text, but a new subclause added
<b>Consequences if not approved:</b>	⌘ <del>Hole in the spec</del> The TS will use a parameter not defined in any specification.

<b>Clauses affected:</b>	⌘ 7.2		
<b>Other specs affected:</b>	<input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘	
<b>Other comments:</b>	⌘		

### How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: [http://www.3gpp.org/3G\\_Specs/CRs.htm](http://www.3gpp.org/3G_Specs/CRs.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.

## 7.2A.3 Tokenized-by parameter definition

### 7.2A.3.1 Introduction

The tokenized-by parameter is an extension parameter appended to encrypted entries in various SIP headers as defined in subclause 5.3.3.1.

### 7.2A.3.2 Syntax

The syntax for the ~~tokenised~~tokenized-by parameter is specified in table ~~x.x.2~~7.6:

**Table 7.6~~x.x.2~~: Syntax of ~~tokenised~~tokenized-by-param**

<code>uri-parameter = transport-param / user-param / method-param / ttl-param / maddr-param / lr-param / tokenized-by-param / other-param <del>tokenised</del>tokenized-by-param = "<del>tokenised</del>tokenized-by" EQUAL hostname</code>
---

The BNF for uri-parameter is taken from IETF RFC 3261 [20] and modified accordingly.

### 7.2A.3.3 Operation

The ~~tokenised~~tokenized-by parameter is appended by I-CSCF(THIG) after all encrypted strings within SIP headers when network configuration hiding is active. The value of the parameter is the domain name of the network which encrypts the information.