3GPP TSG CN Plenary Meeting #16 **NP-020312**
5th - 7th June 2002. Marco Island, USA.

Source: **Lucent Technologies**

Title: **CRs on Asserted Identity**

Agenda item: **8.1**

Document for: **APPROVAL**

Introduction:

This document contains **3** CRs on **Rel-5 on** Work Item **"IMS-CCR"**, that relate to the use of the Asserted-P-Identity header within 3GPP TS 24.229.

These have been discussed by interested parties in a number of conference calls.

TSG CN Plenary meeting #16 is asked for approval.

The revision of CR008 supercedes the version contained in NP-020230.

The revision of CR060 supercedes the version contained in NP-020234.

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	---	---
24.229	008	8	Rel-5	Support for services for unregistered users	B	5.0.0	5.1.0	---	---
24.229	135	1	Rel-5	Asserted identities and privacy	B	5.0.0	5.1.0	---	---

3GPP TSG-CN1 Meeting #23 ***Tdoc N1-02150743211090969106315 10***
Ft. Lauderdale, USA, 8. April - 12. April 2002 *Rev of N1-020863,N1-020905,N1-020957*

CR-Form-v5

CHANGE REQUEST

⌘	24.229	CR	060	⌘ rev	34 89 11	⌘	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 ☒

Title:	⌘	Restructuring of S-CSCF Registration Sections
Source:	⌘	Orange France, Ericsson, Vodafone, dynamicsoft, NEC Corporation, Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	17-May-02
Category:	⌘	**F**
Release:	⌘	Rel-5

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

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. Revision 11 of this CR proposed to provide for the specification of a default public user identity within the P-Associated-URI header. These changes are highlighted in green.		

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 ~~Normal procedures~~Initial registration

~~The S-CSCF shall maintainthree different states for the purpose of user registration, which are:~~

- ~~reg-null state – in this state no REGISTER from a user was received or the user has been de-registered;~~
- ~~reg-await-authentication – in this state an REGISTER message was received from the user and a authentication challenge was sent back to by the S-CSCF. This state is guarded by the reg-await-auth timer;~~
- ~~reg-registered – in this state the user is currently registered.~~

~~In reg-null state, u~~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:

~~Editor's Note: Whether a REGISTER request is initial for an private user identity~~IMPI ~~or an~~ IMPU ~~public user identity needs further discussion.~~

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 ~~from~~ header of the REGISTER request;

2) check if the P-~~3GPP-~~Visisted-Network header is included in the REGISTER request, and if it is included identify the visited network by the value of this header;

~~Editor's Note: The name of and details for the P-3GPP-Visited-Network header needs further clarification.~~

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 thaen zero;~~.~~

4~~3~~) select an authentication vector for the user. If no authentication vector for this user is available, after the S-CSCF ~~shall~~ has performed the Cx Multimedia Authentication procedure with the HSS, as described in 3GPP TS 29.229 [12A], the S-CSCF shall ~~and~~ 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~~<icid> XML element from the message body (see subclause 7.6)~~;

6) remove the p-access-network-info header and may act upon the contents accordingly.

76~~5~~4) ~~request authentication from the UE~~ challenge the user by generating a~~n~~ 401 (~~"~~Unauthorized)~~"~~ response for the receiie~~i~~ved REGISTER request, including a WWW-Authenticate header which transports:

- the ~~private user identity of the user~~ home network identification in the realm field;~~and~~

~~the selected authentication vector, containing~~

- ~~-~~ 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;

- ~~CK -~~ the ~~and~~ IK (Integrity Key) parameters 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);

~~7) informs the HSS that it has been assigned to serve this user by passing its SIP URL to the HSS. This URL shall indicate that the S-CSCF is a loose router, and it may specify the transport protocol and a dedicated port.~~

~~Editor's Note: The detailed coding of the WWW-Authenticate header for the purpose of 3GPP AKA mechanism is ffs.~~

87~~6~~5) - send the so generated 401 (Unauthorized) response towards the UE; and,

98~~7~~6) ~~enter state reg-await-authentication and~~ start timer reg-await-auth which guards the receipt of the next REGISTER request.

~~In reg-await-authentication state,~~ While timer reg-await-auth is running, U~~u~~pon 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 ~~from~~ 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, ~~parameter~~ indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps it the integrity check parameter is included;

~~Editor's Note: The detailed coding of the integrity check parameter are ffs.~~

4) check whether an Authorization header is included, containing:

- the private user identity of the user in the username field; ~~and~~
- 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 ~~during the Cx Authentication procedure~~. The S-CSCF shall only proceed with the following steps if RES and XRES are matching;

6) after performing the Cx ~~registration notification~~Server Assignment procedure with the HSS, as described in 3GPP TS 29.229 [12A], ~~The response from the HSS includes~~ store the following information in the local data:

- the list of public user identities associated to the user, ~~which are~~ 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 ~~for the registered~~ of the user including initial Filter Criteria;

7) bind to each non-barred ~~individual~~ registered public user identity all registered contact information ~~under which the public user identity has been registered (either manually by means of a REGISTER message or implicitly upon the registration of another public user identity)~~;

NOTE ~~2~~1: There might be more then 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~~2: 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 ~~optionally~~ adjust the duration of the registration due to local policy;

10) store the icid parameter received in the P-Charging-Vector header~~<icid> XML element from the message body (see subclause 7.6)~~;

11) remove the p-access-network-info header and may act upon the contents accordingly.

12~~10~~) 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. Using information supplied by the HSS, the P-Associated-URI header will indicate the default public user identity to be used by the P-CSCF in conjunction with the procedures for the P-Asserted-Identity header;

Editor's~~, with an additional entry~~ ~~when a Path header was included in the received REGISTER request, insert its own FQDN, or IP address, in the form of SIP URL~~ ~~at the top of that~~ ~~list~~ ~~found in the Path header saved from the REGISTER request~~~~which indicates:~~; note: The mechanism for indicating this default public user identity is yet to be agreed.

- ~~the SIP URL identifying the S-CSCF; and,~~

- ~~an indication that requests routed in this direction of the path (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 Path header parameter, a character string in the user part or be a port number;~~

- 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;

~~Editor's Note: The above statement shall be aligned to the outcome of the IETF Service-Route discussion / draft.~~

132~~1~~) ~~send~~ the so created 200 (OK) response to the UE;

143~~2~~) 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.

154~~3~~) ~~enter state reg-registered and remain in it for the~~ handle the user as registered for the duration ~~of the registration~~indicated in the Expires header.

5.4.1.2.2 User-initiated reregistration

~~In reg-registered state,~~ U~~u~~pon 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, ~~parameter~~ indicating that the REGISTER request was received integrity protected. The S-CSCF shall only proceed with the following steps i~~f~~t the ~~integrity check parameter is included~~field is set to yes;

~~Editor's Note: The detailed coding of the integrity check parameter are ffs.~~

3) check if~~, due to local policy~~ the user needs to be ~~reregistered or~~ reauthenticated. ~~.~~

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

If the user needs to be ~~reregistered or~~ reauthenticated, the S-CSCF shall proceed with the procedures as described for the initial REGISTER in subclause 5.4.1.2.1~~reg-null state within this section~~, beginning with step ~~4~~3). If the user does not need to be ~~reregistered or~~ reauthenticated, the S-CSCF shall proceed with the following steps in this paragraph; ~~and~~.

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 ~~section~~ 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~~reg-await-authentication state within this section~~, beginning with step 7)~~.~~; and

5) remove the p-access-network-info header and may act upon the contents accordingly.

~~When the S-CSCF receives a REGISTER request, the S-CSCF shall verify that the "path" option-tag is contained in the Proxy-Require header. If the "path" option-tag is present, the S-CSCF shall store the information contained in the Path header so that it can be used for mobile terminated requests.~~

~~Editor's Note: If the S-CSCF receives a Path header without the "path" option tag in the Proxy-Require header, we have an error condition in the I-CSCF. The I-CSCF behavior for this scenario is FFS.~~

~~The S-CSCF shall:~~

- ~~check the existence of a Path header in the request;~~

~~Editor's note: The action S-CSCF has to take when a Path header is not present in the request is FFS.~~

- ~~when a Path header exists in the request, insert its own FQDN, or IP address, in the form of SIP URL at the top of the list found in the Path header saved from the REGISTER request;~~

- ~~save the Contact header value for the entire duration of the registration;~~

- ~~construct a list of preloaded Route headers from the list of entries in the Path header. The order in the lists is preserved;~~

- ~~include an expiration time in the 200 OK response, 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;~~

- ~~save the list of preloaded Route headers for the entire duration of the registration;~~

~~NOTE 1: If this registration is a reregistration, then a list of pre-loaded Route headers will already exist. The new list replaces the old list.~~

- ~~bind to each individual public user identity all contact information under which the public user identity has been registered (either manually by means of a REGISTER message or automatically upon the registration of another public user identity);~~

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

- ~~bind to each contact information the respective Path header entries, that were received in the same REGISTER message as that contact information;~~

- ~~add its Path header on the top of the received list of Path headers, and returns this list in the 200 OK response;~~

- ~~check whether the message contains information indicating that it was received with a valid integrity check by the P-CSCF; and~~

~~Editor's Note: The method by which the P-CSCF indicates this is FFS.~~

- ~~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.~~

~~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.~~

~~The S-CSCF may require authentication of the user for any REGISTER request, and shall always require authentication for initial registration. The information that a REGISTER has a valid integrity check may be used as part of the decision to authenticate the registration. The S-CSCF shall request authentication by responding to the REGISTER request with a 401 Unauthorized with:~~

- ~~the Authorization header containing the authentication parameters (RAND, AUTN, CK and IK).~~

5.4.1.2.3~~2~~ 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~~.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.

Budapest, Hungary, 13. – 17. May 2002

CR-Form-v5

CHANGE REQUEST

⌘ **24.229** **CR** **008** ⌘ **rev** **8** ⌘ 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 ☒

Title:	⌘	Support for services for unregistered users
Source:	⌘	Ericsson, Lucent, Siemens, Nortel, Vodafone
Work item code:	⌘	IMS-CCR
Date:	⌘	15-May-02
Category:	⌘	**B**
Release:	⌘	REL-5

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

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

Reason for change:	⌘	Alignment with stage 2 specifications regarding support for services for unregistered users
Summary of change:	⌘	Procedures at the I-CSCF and S-CSCF are modified to cover the described case
Consequences if not approved:	⌘	Non existent stage 3 procedures describing the support for services for unregistered users

Clauses affected:	⌘	5.3.2.1, 5.4.3.2
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	Revision 4 of this CR was created to incorporate to section 5.4.3.2 the interactions due to CRs 12, 13, 18, 31, 60, 62, 73. Therefore, implementation of clause 5.4.3.2 should be taken from this CR and ignored from the said CRs. Other subclauses modified by these CRs shall be implemented as is. Revision 6 of this CR was created to incorporate to section 5.4.3.2 the interactions due to CRs 094, 095, 096. Therefore, implementation of clause 5.4.3.2 should be taken from this CR and ignore from the said CRs. Other subclauses modified by these CRs shall be implemented as is. Revision 7 of this CR was created to incorporate changes relating to the addition of the p-access-network-info header. Revision 8 of this CR was created to incorporate changes relating to the addition of the P-Asserted-Identity header. These changes are highlighted in green.

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. 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.

Introduction

3GPP TS 23.228 v5.3.0 defines in clause 5.12.1 the *Mobile terminating call procedures to unregistered IMS subscriber that has services to unregistered state.*

However, 3GPP TS 24.229 does not reflect any of the stage 2 procedures. This CR implements the above mentioned stage 2 procedures in 3GPP TS 24.229

Proposed changes

********* First proposed change ***************

5.3.2 Further initial requests

5.3.2.1 Normal procedures

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

When the I-CSCF receives an initial request, not containing a Route header, 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, when the response contains the URL of the assigned S-CSCF ~~information about the required S-CSCF capabilities~~, the I-CSCF shall:

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

2) store the value of the <icid> XML element, if present, 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;

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

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

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

1) select a S-CSCF according to the method described in 29.228 [12]~~that fulfils the indicated mandatory capabilities – if more then one S-CSCFs fulfils the indicated mandatory capabilities the S-CSCF which fulfils most of the possibly additionally indicated optional capabilities~~;

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

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

4~~3~~) forward the request to the selected S-CSCF.

Upon an unsuccessful user location query ~~(e.g., when the response from the HSS indicates that the user does not exist or the user is not registered and no services are provided)~~, the I-CSCF shall ~~:~~

1) return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) or 604 (Does not exist anywhere) in the case the user is not a user of the home network.

The response may be a 480 (Temporarily unavailable) if the user is recognized as a valid user, but is not registered at the moment and it does not have services for unregistered users.

Upon an unsuccessful user location query (e.g.,when the response from the HSS indicates that the user does not exist or the user is not registered and no services are provided for such a user), the I-CSCF shall:

1) return an appropriate unsuccessful SIP response. This response may be a 404 (Not found) or 604 (Does not exist anywhere) in the case the user is not a user of the home network. Thise response may be a 480 (Temporarily unavailable) if the user is recognized as a valid user, but is not registered at the moment and it does not have services for unregistered users.

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

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

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

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

********* Next proposed change ***************

5.4.3.2 Requests terminated at the served user

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

- remove its own URL from the topmost Route header;
- if the S-CSCF does not have the user profile, then initiate the S-CSCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informing the HSS that the user is unregistered, but this S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [12];
- keep the user registration status as unregistered for the duration of the dialog. When the dialog expires, the S-CSCF shall inform appropriately the HSS according to the procedures described in 3GPP TS 29.228 [12];
- check whether the initial request matches the initial filter criteria for unregistered user 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).

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

  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; and

- 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;

- forward the request based on the topmost Route header.

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

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

2) check if P-Original-Dialog-ID header<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-tag, od-from-tag and od-call-id parameter <od-to-tag>, <od-from-tag> and <od-call-id> XML element values from the P-Original-Dialog-ID header<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 P-Original-Dialog-ID header<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 outremove the P-Original-Dialog-ID header<original-dialog-id> XML element from the payload of the request;

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

   a) insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and

   b) initialise local data to track the status of contacting each application server specified in the service profile. Additionally S-CSCF shall also populate the P-Original-Dialog-ID header<original-dialog-id> XML element in the message body with the original To tag, From tag and Call-ID headers received in the request. See subclause 5.4.3.3 for further information on the original dialog identifier.

4) insert a P-Charging-Function-Addresses header (see subclause 7.2.4) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards ASinsert a <charging-function-addresses> XML element in the message body (see subclause 5.4.3.4) populated with values received from the HSS if the message is forwarded within the S-CSCF home network, including towards AS;

54) store the value of the <icid> XML element parameter received in the message body (see subclause 7.6)P-Charging-Vector header and retain the <icid> XML elementparameter in the message bodyP-Charging-Vector header;

6) store the value of the ioi-originating parameter received in the P-Charging-Vector header, if present. The ioi-originating parameter identifies the sending network of the request message. The ioi-originating parameter shall only be retained in the P-Charging-Vector header if the next hop is to an AScheck if <ioi> XML element is present in the payload of the incoming request. If present, the <ioi-originating> child element identifies the sending network of the request message. Store the value of the <ioi-originating> child element received in the message body (see subclause 7.6) and only retain the <ioi> XML element in the message body if the next hop is an AS;

75) 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;

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

9~~6~~) ~~-~~ 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~~;

10) build a Request-URI with the contents of the saved Contact URL determined in the previous step;~~7) - build the Request-URI and Request header field values from the preloaded routes and saved Contact URL, as described in RFC 2543bis [20];~~

11~~8~~) ~~-~~ insert a P-Called-Party-ID SIP header field including the Request-URI received in the INVITE;

12~~9~~) ~~-~~ in case of an initial request for a dialog create a Record-Route header containing its own SIP URL and save the necessary Record-Route header fields and the Contact header field from the request ~~(and from its appropriate responses)~~ in order to release the dialog when needed; ~~and~~

13) optionally, apply any privacy required by draft-peterson-sip-privacy-longterm [27A] to the P-Asserted-Identity header; and

NOTE: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by draft-peterson-sip-privacy-longterm [27A].

~~10) - replace the Request-URI with the contents of the user Contact URL saved by the S-CSCF at registration time; and~~

14~~311~~) ~~-~~ forward the request based on the topmost Route header.

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

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

~~2) execute the procedure described in step 2 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction);~~

2) if the S-CSCF does not have the user profile, then initiate the S-CSCF Registration/deregistration notification with the purpose of downloading the relevant user profile (i.e. for unregistered user) and informing the HSS that the user is unregistered, but this S-CSCF will assess triggering of services for the unregistered user, as described in 3GPP TS 29.228 [12];

3) keep the user registration status as unregistered for the duration of the dialog. When the dialog expires, the S-CSCF shall inform appropriately the HSS according to the procedures described in 3GPP TS 29.228 [12];

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

~~;check whether the initial request matches the initial filter criteria for unregistered user 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).~~

In case that no AS needs to be contacted, then S-CSCF shall return an appropriate unsuccessful SIP response. This response may be a 480 (Temporarily unavailable) and terminate these procedures; and~~In case of contacting one or more application server(s) the S-CSCF shall:~~

~~5.a) insert the AS URL to be contacted into the Route header as the topmost entry followed by its own URL; and~~

~~5.b) 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.~~

5) execute the procedures described in the steps 5~~4~~, 6, 11~~8~~, 12~~9~~, 13 and 14~~31~~ in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction);

~~7) execute the procedure described in step 8 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction);~~

~~8) execute the procedure described in step 9 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction); and~~

~~9) execute the procedure described in step 11 in the above paragraph (when the S-CSCF receives, destined for the registered served user, an initial request for a dialog or a request for a standalone transaction);~~

When the S-CSCF receives a response to the initial request for a dialog (whether the user is registered or not), it shall save the necessary Record-Route header fields and the Contact header field from the response in order to release the dialog if needed. In the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URL contained in the received P-Asserted-Identity header, the S-CSCF shall add a second P-Asserted-Identity header containing this tel-URI, in the case where the network operator has policy to provide privacy on To headers, and such privacy is required for this dialog, change the To header to "Anonymous". Network policy may also require the removal of the display field.

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

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

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

3) remove the p-access-network-info header, if it is present, and may act upon it's contents accordingly; and

~~4~~3) ~~-~~ forward the request based on the topmost Route header.

When the S-CSCF receives a response to the refresh request for a dialog (whether the user is registered or not), it shall save the necessary Record-Route header fields and the Contact header field from the response in order to release the dialog if needed.

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

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

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

3GPP TSG-CN1 Meeting #24
Budapest, Hungary, 13. – 17. May 2002

Tdoc N1-02xxxx

was Tdoc N1-021358

CR-Form-v5

CHANGE REQUEST

⌘ **24.229** **CR** **135** ⌘ **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 [X] ME/UE [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Asserted identities and privacy
Source:	⌘	Lucent Technologies
Work item code:	⌘	IMS-CCR
Date:	⌘	11/05/02
Category:	⌘	**B**
Release:	⌘	Rel-5

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

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

Reason for change: ⌘ The provision of mechanisms to allow the IM CN subsystem to present an calling identity to the called user, and for the calling user to restrict such identity, as provided in the stage 1 description 3GPP TS 22.228. This CR proposes the usage of a number of recent drafts to provide such mechanisms.

Summary of change: ⌘ For requests.

The Assserted-Identity may optionally be provided by the UE. It is optional because the IETF procedures only provide for a hint. If provided it is a public user identity.

The P-CSCF asserts this identity. If an identity is not provided then the P-CSCF has to assign a default from among the known registered public user identities associated with this security domain. This is currently based on best knowledge within the P-CSCF but we may wish to provide some information from S-CSCF to P-CSCF at registration time that indicates this. The S-CSCF and AS may use this P-Asserted-Identity to identify the user.

The remote S-CSCF implements any privacy requirements.

The P-Asserted-Identity can be provided to the remote user if privacy requirements are met. For dial-back requirements (which are normally required for CLIP), the UE will need to decide between the Reply-To header versus the P-Asserted-Identity. The P-Asserted-Identity will not necessarily provide a URL where calls can be received.

For responses similar procedures to the above apply. Note that the P-Asserted-Identity is only to appear in 1xx or 2xx responses, but privacy of this header will be applied to all responses.

		This CR does not yet provide changes required for procedures in the MGCF, nor does it yet provide changes for the profile in Annex A, nor does it provide any inclusion of the unapproved drafts in annexes to 24.229.
Consequences if not approved:	⌘	No identity services will be available in Release 5

Clauses affected:	⌘	2, 4.4 (new), 5.1.2A (new), 5.2.2, 5.2.6.2, 5.2.6.3, 5.4.3.1, 5.5.3.1.1, 5.5.3.1.2, 5.5.3.2.2, 5.6.2, 7.2.7 (new), A.2.1.2, A.2.2.2
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	Revision 1 of this CR created as a result of the discussions of a conference call held on 23rd May 2002 and a subsequent conference call held on 31st May 2002. The following agreements were made at these calls:

1. Name of the header looks like it will be P-Asserted-Identity for both the hint and the value within the trusted domain.

2. The local P-CSCF is the entity responsible for applying the assertion, and therefore for processing any hint into an asserted identity.

3. The hint should be a public user identity. A discussion as to whether it should be mandatory or not resolved that the P-CSCF should have a default public user identity. If the user required a service profile and public user identity different from that provided as the default, then it was mandatory for the UE to insert the public user identity. If the user required a service profile and public user identity the same as the default, then it was optional for the UE to insert the public user identity.

4. The default public user identity should be sourced from the HSS at registration time. It was agreed that the appropriate way of doing this was by means of some form of parameter within the URI of the Associated-URI list that related to the default URI. It was agreed that the best way of doing this would be discussed on the email list. This mechanism had the advantage that it would probably require no amendments to the Cx interface protocol.

5. The asserted identity was appropriate to all requests for an initial request for a dialog and a standalone transaction. It was agreed that a special case did not need to be made for NOTIFY request as response to a SUBSCRIBE request as the asserted identity would be in the 2xx response to the SUBSCRIBE request, and although due to transmission delays this would arrive later, this would not be an issue.

6. The asserted identity was appropriate to 18x and 2xx responses to an initial request for a dialog and a standalone transaction.

7. No hint would be provided for within responses. It was considered not useful. If provided it would be ignored (although the value supplied could be the one eventually used because it was the one in the request-URI). This was after a discussion of the appropriate service profile to provide at the destination side, and it was agreed that this would always be the one identified in the Request-URI.

8. The contents of the From and To headers have no impact on the operation of the P-Asserted-Identity. These values do not form any part of the hint, or the determination of the P-Asserted-Identity.

9. The UE optionally provides an indication of privacy or no privacy.

10. The local S-CSCF provides an indication of privacy or no privacy from the service profile if not provided by the UE. It is mandatory that the service profile contains such a value.

11. There was discussion about which entity should implement the privacy. The working assumption was that it should be the last entity in the trust domain, be it P-CSCF, I-CSCF, MGCF, BGCF or S-CSCF. It was also considered appropriate that the remote S-CSCF may also apply the privacy as a matter of local policy to that network. It was considered that the last entity in the trust domain would be an implementation of what was in the internet-draft, and therefore possibly did not need to be duplicated in the text of 24.229. The proposed 4.4 text of the CR in N1-021358 covers this.

12. The CR allows the S-CSCF at the sending side to modify the contents of the From (and To) headers based on the contents of the Privacy header. This is a network provider policy option, and therefore it is not guaranteed to occur (and therefore there is a need for the user to provide his own privacy on this space). It is network provider policy whether this also impacts the display field within these headers or not. Network provider policy will obviously need to reflect the needs of regulators for the network provider's. Note that there are interoperability issues with implementations of RFC2543, but it is believed that these scenarios will not occur within the IM CN subsystem usage.

13. The new clause 4.4 reflects the extent of the trust domain. Application servers of third-party service providers are outside the trust domain. Certain UAs are also in the trust domain. Additionally, text is included within that for the BGCF, but only relating to INVITEs.

14. Where a tel-url and a sip-url are associated, and the S-CSCF receives one from the P-CSCF, then the S-CSCF shall also insert the other. This is to allow the MGCF to receive a tel-url if one exists. The MGCF is not responsible for converting a received sip-url to an equivalent tel-url.

15. In annex A, the major capabilities tables have been included, but have not yet included the PDU tables, which will be the subject of a further CR. The impact of the statements here is that all 3GPP IM CN subsystem entities plus the UE need to support both extensions.

The changes in subclause 5.2.6.3 assume the approval of CR095 to 24.229, and therefore the text is provided in accordance with this CR, rather than in accordance with the structure of the existing text before modification.

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. Below is a brief summary:

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

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

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

FIRST PROPOSED CHANGE

2 References

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

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

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

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

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

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

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

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

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

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

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

[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".

[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-ietf-sip-asserted-identity~~draft-jennings-sipping-nai~~-00~~draft- sip-privacy-03~~ (~~November 2001~~May 2002): "Extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks~~SIP extensions for caller identity and privacy~~".

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

[27A] draft-~~peterson~~ietf-sip-privacy-~~longterm~~general-00 (May 2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

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.

SECOND PROPOSED CHANGE

4.4 Trust domain for asserted identity

draft-ietf-sip-asserted-identity ~~draft-jennings-sipping-nai-00~~ [27] provides for the existence and trust of an asserted identity within a trust domain. For the IM CN subsystem, this trust domain consists of the P-CSCF, the I-CSCF, the S-CSCF, the BGCF, the MGCF, the MRFC, ~~the MGCF~~, and all ASs that are not provided by third-party service providers. ASs provided by third-party service providers are outside the trust domain.

NOTE: In addition to the procedures specified in clause 5, procedures of draft-ietf-sip-asserted-identity [27] in relation to transmission of P-Asserted-Identity headers and their contents outside the trust domain also apply.

THIRD PROPOSED CHANGE

5.1.2.2 General SUBSCRIBE requirements

If the UA receives a 503 Service Unavailable response to an initial SUBSCRIBE request containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

Editor's Note: 5.1.2.3 is reserved for subscription and notification to future events

5.1.2A Generic procedures applicable to all methods

5.1.2A.1 Mobile-originating case

In accordance with draft-ietf-sip-asserted-identity~~draft-jennings-sipping-nai~~ [27] the UE may insert a~~n~~ P-Asserted-Identity header in any initial request for a dialog or request for a standalone transaction as a hint for creation of an asserted identity within the IM CN subsystem. The UE may include any of the following in the P-Asserted-Identity header:

- a public user identity stored in the USIM which has been registered by the user;
- a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implict registration; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current ~~implicit~~ registration.

NOTE 1: The temporary public user identity specified in subclause 5.1.1.1 is not a public user identity suitable for use in the P-Asserted-Identity header.

Where privacy is required, i~~I~~n any initial request for a dialog or request for a standalone transaction, the UE ~~should~~ shall set the From header to "Anonymous".

NOTE 2: It is a matter of network policy as to whether any of the contents of the From header are modified based on any privacy specified by the user either within the UE indication of privacy or by network subscription. Therefore the user could require to include the value "Anonymous" even on requests where privacy is not explicitly requested.

~~NOTE 2: Any value placed in the From header will be automatically transferred to the remote user, and as a result may be known by that user. The IM CN subsystem accepts no responsibility for imposing any privacy on this header value. In particular, any provision of privacy applied to all calls as a subscription arrangement (a condition that might be unknown to the UE) will not be applied to the From header.~~

The UE can indicate privacy of the P-Asserted-Identity in accordance with draft-~~petersonietf~~-sip-privacy-~~longterm~~general [27A], and the additional requirements contained within draft-ietf-sip-asserted-identity [27].

5.1.2A.2 Mobile-terminating case

~~In accordance with draft-jennings-sipping-nai [27] the UE may insert an Asserted-Identity header in any provisional response or 2xx response to an initial request for a dialog, or a 2xx response to a request for a standalone transaction as a hint for creation of an asserted identity within the IM CN subsystem. The UE may include any of the following in the Asserted-Identity header:~~

- ~~a public user identity stored in the USIM which has been registered by the user;~~
- ~~a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implict registration;~~
- ~~any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current implicit registration.~~

The UE can indicate privacy of the P-Asserted-Identity in accordance with draft-~~petersonietf~~-sip-privacy-~~longterm~~general [27A].

NOTE: In the mobile-terminating case, this version of the document makes no provision for the UE to provide an P-Asserted-Identity in the form of a hint.

5.1.3 Call initiation - mobile originating case

Editor's Note: A more detailed description of the INVITE responses (183, 180, 200...) might be needed here.

5.1.3.1 Initial INVITE

3GPP terminals shall indicate the support for reliable provisional responses and specify it using the Supported header mechanism.

5.1.3.2 PRACK

Void.

5.1.3.3 COMET

Void.

5.1.3.4 ReINVITE

Void.

FOURTH PROPOSED CHANGE

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:

- insert a Path header in the request. The P-CSCF shall include in the Path header an entry containing the SIP URL identifying the P-CSCF;
- insert a Require header and a Proxy-Require header both containing the option tag "path";
- 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.

- 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 routeing 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.

5) store the default public user identity for use with procedures for the P-Asserted-Identity. The default public user identity is specifically indicated in the Associated-URI header values.

Editor's note: The exact mechanism for indicating this value is for further discussion.

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 routeing 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.

FIFTH PROPOSED CHANGE

5.2.6.2 Requests initiated by the UE

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains as P-Asserted-Identity header that matchs one of the registered public user identities, the P-CSCF shall identify the initiator of the request by that public user identity.

When the P-CSCF receives an initial request for a dialog or a request for a standalone transaction, and the request contains as P-Asserted-Identity header that does not match one of the registered public user identities, or does not contain a~~n~~ P-Asserted-Identity header, the P-CSCF shall identify the initiator of the request by a default public user identity. ~~The selection of a default public user identity is a matter for the P-CSCF operator, but shall not include any temporary public user identity used for registration from a R99 USIM.~~

NOTE: The contents of the From header do not form any part of this decision process.

When the P-CSCF receives from the UE an initial request for a dialog, and a 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;
- insert a~~n~~ P-Asserted-Identity header with a value representing the initiator of 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 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;
- insert a~~n~~ P-Asserted-Identity header with a value representing the initiator of 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
- insert an P-Asserted-Identity header with a value representing the initiator of the request;
- 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.

5.2.6.3 Requests terminated by the UE

~~When the P-CSCF receives a response to an initial request for a dialog or a response to a request for a standalone transaction, and the response contains as Asserted-Identity header that matchs one of the registered public user identities, the P-CSCF shall identify the responder to the request by that public user identity.~~

When the P-CSCF receives a response to an initial request for a dialog or a response to a request for a standalone transaction~~, and the response contains as Asserted-Identity header that does not match one of the registered public user identities, or does not contain an Asserted-Identity header~~, the P-CSCF shall identify responder by a ~~default~~ public user identity that relates to the Request-URI used in the request~~. The selection of a default public user identity is a matter for the P-CSCF operator, but shall not include any temporary public user identity used for registration from a R99 USIM.~~

NOTE: The contents of the To header do not form any part of this decision process.

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:

- insert an P-Asserted-Identity header with a value representing the ~~initiator of~~ responder to the request;
- 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:

- insert an P-Asserted-Identity header with a value representing the ~~initiator of~~ responder to the 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 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 receives, destined for the UE, a subsequent request for a dialog that is not a refresh request, 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~~ parameter from ~~the message body~~ P-Charging-Identity header (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.

SIXTH PROPOSED CHANGE

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

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;
- in the case where the S-CSCF has knowledge of an associated tel-URI for a SIP URL contained in the received P-Asserted-Identity header, add a second P-Asserted-Identity header containing this tel-URI;
- in the case where the network operator has policy to provide privacy on From headers, and such privacy is required for this dialog, change the From header to "Anonymous". Network policy may also require the removal of the display field;
- 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 any response to the above request, the S-CSCF ~~shall~~may:

- apply any privacy required by draft-~~petersonietf~~-sip-privacy-~~longterm~~general [27A] to the P-Asserted-Identity header.

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

NOTE 2: The optional procedure above is in addition to any procedure for the application of privacy at the edge of the trust domain specified by draft-~~peterson~~ietf-sip-privacy-~~longterm~~general [27A].

When the S-CSCF receives from the served usera 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.

SEVENTH PROPOSED CHANGE

5.5 Procedures at the MGCF

5.5.1 General

The MGCF, although acting as a UA, does not initiate any registration of its associated addresses. These are assumed to be known by peer-to-peer arrangements within the IM CN subsystem. Therefore the dependencies of table 0.3/1 and table 0.3/2 shall not apply.

The use of the Path header shall not be supported by the MGCF.

5.5.2 Subscription and notification

5.5.2.1 Subscriptions to MGCF events

Void.

5.5.2.2 Gateway behaviour for SUBSCRIBE / NOTIFY

Void.

5.5.3 Call initiation

5.5.3.1 Initial INVITE

5.5.3.1.1 Calls originated from circuit-switched networks

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

- generate and send an INVITE request:
  - set the Request-URI to the "tel" format using an E.164 address;
  - set the Supported header to "100rel" (see draft-ietf-sip-manyfolks-resource [22]); ~~and~~
  - include an P-Asserted-Identity header; and
  - create a new, globally unique value for the <icid> XML element and insert it into the message body (see subclause 7.6).

5.5.3.1.2 Calls terminating in circuit-switched networks

When the MGCF receives an initial INVITE request, the MGCF shall:

- send 100 "Trying" response;
- assuming the "100rel" indicator was received and a matching codec is found,send 183 "Session Progress" response:
  - set the Require header to the value of "100rel";
  - set the Content-Disposition header to the value of "precondition"; ~~and~~
  - include an P-Asserted-Identity header; and
  - store the value of the <icid> XML element received in the message body (see subclause 7.6).

Editor's note: must receive Supports header with value of 100rel in the INVITE.

Editor's note: need text to describe error legs.

5.5.3.2 Subsequent requests

5.5.3.2.1 Calls originating in circuit-switched networks

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

- send a COMET request.

5.5.3.2.2 Calls terminating in circuit-switched networks

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

- send 180 "Ringing" to the UE.

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

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

SEVENTH PROPOSED CHANGE

5.6 Procedures at the BGCF

5.6.1 General

The use of the Path header shall not be supported by the BGCF.

5.6.2 Session initiation transaction

When the BGCF receives an INVITE request, the BGCF shall forward the request either to an MGCF within its own network, or to another network containing an MGCF. The BGCF need not Record-Route the INVITE request. While the next entity may be a MGCF acting as a UA, the BGCF shall not apply the procedures of draft-petersonietf-sip-privacy-longtermgeneral [27A] relating to privacy. The BGCF shall 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.

NOTE: The means by which the decision is made to forward to an MGCF or to another network is outside the scope of the present document, but may be by means of a lookup to an external database, or may be by data held internally to the BGCF.

EIGHTH PROPOSED CHANGE

7.2.7 P-Asserted-Identity header

7.2.7.1 Introduction

The P-Asserted-Identity header is the mechanism whereby the first element in the trust domain (see subclause 4.4) may assert a public user identity identifying the user. The P-Asserted-Identity header can also be used as a hint to the first element in the trust domain when it selects the asserted public user identity.

The header is inserted at the first opportunity when initialising dialogs and with standalone transactions. The header may be included in requests and responses.

7.2.7.2 Syntax

The P-Charging-Function-Addresses header field has the syntax described in draft-ietf-sip-asserted-identity [35].

7.2.7.3 Operation

The operation of this header is described in clause 5.

NINTH PROPOSED CHANGE

5.8.2 Call initiation

5.8.2.1 Initial INVITE

5.8.2.1.1 MRFC-terminating case

The MRFC shall provide a P-Asserted-Identity header in a response to the initial request for a dialog, or any response for a standalone transaction. It is a matter of network policy whether the MRFC expresses privacy according to draft-ietf-sip-privacy-general [27A] with such responses.

When the MRFC receives an initial INVITE request, the MRFC shall store the value of the <icid> XML element received in the message body (see subclause 7.6).

5.8.2.1.1.1 Tones and announcements

The MRFC can receive INVITE requests to set up a session to play tones and announcements. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator for a tone or announcement, the MRFC shall:

- send 100 Trying response.

Editor's note: it is FFS how to identify the tone or announcement to be played.

5.8.2.1.1.2 Ad-hoc conferences

The MRFC can receive INVITE requests to set up an ad-hoc conferencing session (e.g. Multiparty Call) or to add parties from the conference. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator to initiate ad hoc conferencing, the MRFC shall:

- send 100 Trying response; and
- after the MRFP indicates that the conference resources are available, send 200 OK response with an MRFC conference identifier.If the MRFC chooses to send a 183 Session Progress response prior to the 200 OK, then the conference identifier may also be included in the 183 Session Progress response.

When the MRFC receives an INVITE request with an indicator to add a party to an existing ad hoc conference (i.e. MRFC conference identifier), the MRFC shall:

- send 100 Trying response; and
- after the MRFP indicates that the conferencing request is granted, send 200 OK response with the MRFC conference identifier.If the MRFC chooses to send a 183 Session Progress response prior to the 200 OK, then the conference identifier may also be included in the 183 Session Progress response.

Editor's note: it is FFS how to identify the resources of the MRFC/MRFP.

5.8.2.1.1.3 Transcoding

The MRFC may receive INVITE requests to set up transcoding between endpoints with incompatible codecs. The MRFC acts as terminating UA in this case.

When the MRFC receives an INVITE request with an indicator for transcoding and a codec is supplied in SDP, the MRFC shall:

- send 100 Trying response; and
- after the MRFP indicates that the transcoding request is granted, send 200 OK response.

When the MRFC receives an INVITE request with an indicator for transcoding but no SDP, the MRFC shall:

- send 183 Session Progress response with list of codecs supported by the MRFC/MRFP.

5.8.2.1.2 MRFC-originating case

~~Void.~~The MRFC shall provide a P-Asserted-Identity header in an initial request for a dialog, or any request for a standalone transaction. It is a matter of network policy whether the MRFC expresses privacy according to draft-ietf-sip-privacy-general [27A] with such requests.

TENTH PROPOSED CHANGE

A.2.1.2 Major capabilities

Table A.3: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
1	client behaviour for registration?	[20]	m	m
2	server behaviour for registration?	[20]	n/a	n/a
3	registrar?	[20]	n/a	n/a
4	client behaviour for session requests?	[20]	m	o
5	server behaviour for session requests?	[20]	m	o
6	session release?	[20]	m	c1
7	timestamping of requests?	[20]	o	o
8	authentication between UA and UA?	[20] subclause 22.4	o	o
9	authentication between UA and registrar?	[20] subclause 22.4	o	n/a
10	insertion of date in requests and responses?	[20] subclause 24.17	o	o
11	downloading of alerting information?	[20] subclause 22.4	o	o
	Extensions			
12	The SIP INFO method?	[19]	o	n/a
13	Reliability of provisional responses in SIP?	[21]	o	m
14	SIP caller preferences and callee capabilities?	[24]	o	o
15	the REFER method?	[25]	o	o
16	The SIP session timer?	[26]	o	o
17	Integration of resource management and SIP?	[22]	o	m
18	SIP extensions for caller identity and privacy?	[27]	o	m
19	SIP extensions for supporting distributed call state?	[28]	o	o
20	SIP extensions for media authorization?	[29]	o	m
21	SIP specific event notification	[23]	o	o
22	acting as the notifier of event information	[23]	c2	c2
23	acting as the recipient of event information	[23]	c2	c2
24	extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks	[27]	o	m
25	a Privacy Mechanism for the Session Initiation Protocol (SIP)	[27A]	o	m
c1: IF A.3/4 OR A.3/5 THEN m ELSE o. c2: IF A.3/21 THEN o.1 ELSE n/a. o.1: At least one of these capabilities is supported.				

NINTH PROPOSED CHANGE

A.2.2.2 Major capabilities

Table A.150: Major capabilities

Item	Does the implementation support	Reference	RFC status	Profile status
	Capabilities within main protocol			
1	client behaviour for registration?	[20]	m	m
2	server behaviour for registration?	[20]	m	m
3	registrar?	[20]	o	
4	client behaviour for session requests?	[20]	m	m
5	server behaviour for session requests?	[20]	m	m
6	session release?	[20]	m	m
7	Stateless proxy behaviour?	[20]	o.1	
8	Stateful proxy behaviour?	[20]	o.1	
9	insertion of date in requests and responses	[20] 24.17	o	o
10	suppression or modification of alerting information data	[20] 22.4	o	o
11	reading the contents of the Require header before proxying the request or response	[20] 24.33	o	o
12	adding or modifying the contents of the Require header before proxying the REGISTER request or response	[20] 24.33	o	m
13	adding or modifying the contents of the Require header before proxying the request or response for methods other than REGISTER	[20] 24.33	o	o
14	reading the contents of the Supported header before proxying the response	[20] 24.39	o	o
15	reading the contents of the Unsupported header before proxying the 420 response to a REGISTER	[20] 24.42	o	m
16	reading the contents of the Unsupported header before proxying the 420 response to a method other than REGISTER	[20] 24.42	o	o
17	the inclusion of the Error-Info header in 3xx - 6xx responses	[20] 24.42	o	o
	Extensions			
18	The SIP INFO method?	[19]	o	o
19	Reliability of provisional responses in SIP?	[21]	o	m
20	SIP caller preferences and callee capabilities?	[24]	o	o
21	the REFER method?	[25]	o	o
22	The SIP session timer?	[26]	o	o
23	Integration of resource management and SIP?	[22]	o	m
24	SIP extensions for caller identity and privacy?	[27]	o	m
25	SIP extensions for supporting distributed call state?	[28]	o	o
26	SIP extensions for media authorization?	[29]	o	m
27	SIP specific event notification	[23]	o	o
28	extensions to the Session Initiation Protocol (SIP) for Network Asserted Identity within Trusted Networks	[27]	o	m
29	a Privacy Mechanism for the Session Initiation Protocol (SIP)	[27A]	o	m
o.1:	It is mandatory to support at least one of these items.			