3GPP TSG SA WG3 Security — S3#23 **S3-020328**
9 - 12 July 2002
Helsinki, Finland

3GPP TSG-CN1 Meeting #24 ***Tdoc N1-021427***
Budapest, Hungary 13-17. May 2002

Title:	Response Liaison Statement on IMS Identities for R99/R4 UICC
Source:	CN1
To:	SA1, SA2
Cc:	SA3, CN4, T3
Response to:	LS (S1-020871) on SA1 Assumptions on IMS identities and UICCs; and LS (S2-021526) on IMS Identities for Rel 99/R4 UICC from SA2.

Contact Person:
Name: Andrew Allen
Tel. Number: +1 972 473 5507
E-mail Address: aallen@dynamicsoft.com

Attachments: N4-020774, N1-021405, N1-021424, N1-021441

---

1. Overall Description:

CN1 thanks SA1 and SA2 on their Liaison Statements concerning the identity requirements for access to IMS with a R99/Rel-4 UICC.

CN1 would like to inform SA1 and SA2 that CN1 has approved CRs to IMS specifications TS 23.218 and TS 24.229 to implement the stage 2 requirements for Temporary Public User Identities and barred public user identities contained in the SA2 CRs to TS 23.228. CN1 has also discussed and agreed a CR to TS 23.003 that defines the format for the R99/Rel 4 UICC for Home Domain name, Private User Identity and Public User Identity based on the content of the discussion paper attached to the SA2 LS and forwarded this CR to CN4 where it was agreed as N4-020774.

CN1's understanding of CR 154 (S2-021525) and CR 155 (S2-021344) to TS 23.228 concerning barred public user identities is that services are never executed for session requests originated from or terminated to barred public user identities. The S-CSCF therefore will always return a 4XX response to any request (other than REGISTER) originated from or terminated to a barred public user identity before any match is made of triggers in the initial filter criteria. This means that an Application Server cannot be contacted for a session request from or to a barred public user identity.

2. Actions To SA2:

To confirm that the S-CSCF should always return a 4XX response to any request (other than REGISTER) originated from or terminated to a barred public user identity before any match is made of triggers in the initial filter criteria.

3. Date of Next CN1 Meetings:

CN1_25	29th July – 02nd August 2002	Helsinki, Finland

3GPP TSG CN WG4 Meeting #14 ***N4-020774***
Budapest, Hungary, 13th – 17th May 2002 **revision of N1-021445 (N4-020757)**

3GPP TSG-CN1 Meeting #24 ***Tdoc N1-021461***
Budapest, Hungary, 13. – 17. May 2002 **revision of N1-021445 (N1-021329)**

CR-Form-v5

CHANGE REQUEST

⌘ **23.003** **CR** **041** ⌘ **rev** **2** ⌘ Current version: **5.2.0** ⌘

*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 **X** Radio Access Network ☐ Core Network **X**

Title:	⌘	Use of a temporary public user identity
Source:	⌘	Vodafone, Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	1st May 2002
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:	⌘	SA2 have agreed the stage two for IMS access with a R99/Rel-4 USIM. In order to align with the stage two, it is now necessary to add the procedures to derive domain name, private user identity and public user identity from the IMSI.
Summary of change:	⌘	Addition of conversion procedures in a new section on IMS.
Consequences if not approved:	⌘	Pre-Release-5 USIMs not supported by IMS

Clauses affected:	⌘	
Other specs affected:	⌘	☐ Other core specifications ⌘
		☐ Test specifications
		☐ O&M Specifications
Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/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.

1.1 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 TS 21.905: "3G Vocabulary".

[2] 3GPP TS 23.008: "Organization of subscriber data".

[3] Void.

[4] 3GPP TS 23.070: "Routeing of calls to/from Public Data Networks (PDN)".

[5] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[6] 3GPP TS 29.060: "GPRS Tunnelling protocol (GPT) across the Gn and Gp interface".

[7] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[8] GSM 09.03: "Digital cellular telecommunications system (Phase 2+); Signalling requirements on interworking between the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN) and the Public Land Mobile Network (PLMN)".

[9] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[10] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[11] ITU-T Recommendation E.212: "The international identification plan for mobile terminals and mobile users".

[12] ITU-T Recommendation E.213: "Telephone and ISDN numbering plan for land Mobile Stations in public land mobile networks (PLMN)".

[13] ITU-T Recommendation X.121: "International numbering plan for public data networks".

[14] RFC 791: "Internet Protocol".

[15] RFC 1883: "Internet Protocol, Version 6 (IPv6) Specification".

[16] 3GPP TS 25.401: "UTRAN Overall Description".

[17] 3GPP TS 25.413: "UTRAN Iu Interface RANAP Signalling".

[18] RFC 2181: “Clarifications to the DNS Specification”.

[19] RFC 1035: “Domain Names - Implementation and Specification”.

[20] RFC 1123: “Requirements for Internet Hosts -- Application and Support”.

[21] 3GPP TS 23.236: "Intra Domain Connection of RAN Nodes to Multiple CN Nodes".

[22] 3GPP TS 23.228: "IP Multimedia (IM) Subsystem – Stage 2"

[23] RFC 2486: "The Network Access Identifier"

[24] RFC 3261: "SIP: Session Initiation Protocol"

[25] 3GPP TS 31.102: "Characteristics of the USIM Application."

[26] RFC 1035: "Domain names – imnplementation and specification"

*** Proposed New Section ***

13 Numbering, addressing and identification within the IP multimedia core network subsystem

13.1 Introduction

This clause describes the format of the parameters needed to access the IP multimedia core network subsystem. For further information on the use of the parameters see 3GPP TS 23.228 [22].

13.2 Home network domain name

The home network domain name shall be in the form of an Internet domain name, e.g. operator.com, as specified in RFC 1035 [26].

If there is no ISIM application, the UE shall derive the home network domain name from the IMSI as described in the following steps:

~~1. remove any non-decimal digits from the IMSI, leaving a string of 15 or less digits;~~

~~2~~1. take the first 5 or 6 digits, depending on whether a 2 or 3 digit MNC is used (see 3GPP TS 31.102 [25]) and separate them into MCC and MNC with "."; and

~~3~~2. reverse the order of the MCC and MNC. Append to the result: ".IMSI.3gppnetwork.org"

An example of a home network domain name is:

EXAMPLE: IMSI in use: 234150999999999;

where;

MCC: 234;

MNC: 15;

MSIN: 0999999999; and

home domain name: 15.234.IMSI.3gppnetwork.org.

13.3 Private user identity

The private user identity shall take the form of an NAI, and shall have the form user@realm as specified in clause 3 of RFC2486 [23].

NOTE: It is possible for a representation of the IMSI to be contained within the NAI for the private identity.

If there is no ISIM application, the private user identity is not known. In this case, the private user identity is derived from the IMSI.

The following steps show how to build the private user identity out of the IMSI:

~~1. remove any non-decimal digits from the IMSI, leaving a string of 15 or less digits;~~

1~~2~~. use ~~the result from step 1, i.e.~~ the whole string of digits~~,~~ as the user part of the private user identity; and

2~~3~~. the first digits of the IMSI, i.e. MNC and MCC, will be converted into a domain name, as described in subclause 13.2~~1~~.

The result will be a private user identity of the form imsi@mnc.mcc."IMSI.3gppnetwork.org". For example: If the IMSI is 234150999999999 (MCC = 234, MNC = 15), the private user identity then takes the form 234150999999999@15.234.IMSI.3gppnetwork.org

13.4 Public user identity

The public user identity shall take the form of either a SIP URI, see RFC3261[24] or an E.164 number. A SIP URI shall take the form "sip:user@domain".

~~In case~~If there is no ISIM application to host the public user identity, a temporary public user identity shall be derived, based on the IMSI. The temporary public user identity shall be of the form "user@domain" and shall therefore be equal to the private user identity. The private user identity is derived as per subclause 13.2. That is, the private user identity will be appended to the string "sip:"

EXAMPLE: "sip:234150999999999@15.234.IMSI.3gppnetwork.org".

CR-Form-v5

CHANGE REQUEST

⌘ **TS 23.218 CR 003** ⌘ **rev 10** ⌘ Current version: **5.0.0** ⌘

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

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

Title:	⌘	Clarification on SPI related text
Source:	⌘	dynamicsoft, Ericsson
Work item code:	⌘	IMS-CCR
Date:	⌘	2002/05/13
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: ⌘
1) In the current text, default handling procedure is initiated when AS is failed. However, there is no description about the treatment of remaining filter criteria list.
2) Clarify that the S-CSCF downloads and stores the filter criteria (profile subset) from the HSS.
3) Clarify precedence in handling of "barring" versus triggers
4) Delete reference to "refreshing dialogue".

Summary of change: ⌘ **Previous T-doc no at CN1#23: N1-020953; then #23 SIP Ad Hoc 021102**
1) In section 5.2, it is proposed to describe that the default handling procedure will abandon the remaining filter criteria list
2) Confirm that triggers apply solely to dialogue initiation

Consequences if not approved: ⌘
1) Default handling procedure will be implemented wrongly.
2) Possible confusion that triggers apply not only to dialogue initiation

Clauses affected: ⌘ 5.2, 6.4, 6.5, 6.9, 7.2.1, B.3.1

Other specs affected: ⌘
☐ Other core specifications ⌘
☐ Test specifications
☐ O&M Specifications

Other comments: ⌘ Changes done on this CR version:
1) note2 (5.2)
2) barring verification, iFC download, minor edit 1st para. (6.4)
3) deletion of refreshing (6.4, 6.5.1, 6.5.2)
4) verification of barred user (6.5.1, 6.5.2)

	5) reference to XML (6.9.2) 6) Default handling & AS being FFS (6.9.2.2)

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.

Change

5.2 Service interaction with IP multimedia subsystem

Service Points of Interest (SPIs) are those points in the SIP signalling on which Filter Criteria can be set. The following SPIs are defined:

- any initial known or unknown SIP method (e.g. REGISTER, INVITE, SUBSCRIBE, MESSAGE);
- presence or absence of any header;
- content of any header;
- direction of the request is with respect to the served user – either mobile originated (MO) or mobile terminated (MT) or mobile terminated to unregistered user;

  NOTE 1: REGISTER is considered part of the Mobile Origination.

  NOTE 2: The S-CSCF shall verify if the end user is barred before checking if any trigger applies for that end user.

- session description information.

A Filter Criteria triggers one or more SPIs in order to send the related request to one specific application server. The set of Filter Criteria that is stored for a service profile of a specific user is called "Application Server Subscription Information". In order to allow the S-CSCF to handle the different Filter Criteria in the right sequence, a priority shall be assigned to each of them. ~~Additionally Filter Criteria may indicate that a dialog shall be released and abandon the servicing of the remaining list of filter criteria be terminated if the indicated Application Server cannot be reached or the AS requests to perform the default handling procedure.~~ If the S-CSCF can not reach the AS, the S-CSCF shall apply the default handling associated with the trigger. This default handling shall be :

- To continue verifying ~~of~~ if the triggers of lower priority in the list match; or
- To abandon verification of matching of the triggers of lower priority in the list; and to release the dialogue.

Therefore a Filter Criteria shall contain the following information:

- address of the Application Server to be contacted;
- priority of the Filter Criteria providing the sequence in which the criteria shall be applied;
- trigger Points, which indicated the Service Points of Interest (SPIs) triggered by this Filter Criteria. The SPIs may be linked by means of logical expressions (AND, OR, NOT, etc.);
- default ~~H~~handling (as described above). ~~, i.e. indication if the dialog shall be released and abandon the servicing of the remaining list of filter criteria be terminated if the AS cannot be reached or the AS requests to perform the default handling procedure.;~~
- optional Service Information that shall be added to the message body before it is sent to the AS (as an example this may include the IMSI for the IM-SSF).

The same priority shall not be assigned to more than one initial Filter Criteria~~to more than one AS~~) for a given end user. .

In the case that multiple Filter Criteria are sent from the HSS to the S-CSCF when the S-CSCF receives a message via the Mw interface, the S-CSCF shall check the filter criteria one by one according to their indicated priority, i.e. the S-CSCF shall:

1. set up the list of filter criteria for that request according to their priority – the sequence of the filter criteria shall not be changed until the request finally leaves the S-CSCF via the Mw interface again;
2. parse the received request in order to find out the Service Points of Interest (SPIs) that are included in it;
3. check whether the trigger points of the filter criteria with the next highest priority are matched by the SPIs of the request and

a) if it does not match the S-CSCF shall immediately proceed with step ~~6~~ 4;

b) if it matches the S-CSCF shall:

i) add an indication to the request which will allow the S-CSCF to identify the message on the incoming side, even if its dialog identification has been changed e.g. due to the AS performing third party call control;

ii) forward the request via the ISC interface to the AS indicated in the current filter criteria. The AS then performs the service logic, may modify the request and may send the request back to the S-CSCF via the ISC interface;

iii) proceed with step ~~6~~ 4 if the request was received again from the AS via the ISC interface;

4~~6~~. repeat the above steps 2 ~~to 5~~ and 3 for every filter criteria which was initially set up (in step 1) until the last filter criteria has been checked;

5~~7~~. route the request based on normal SIP routing behaviour.

If an Application Server decides to locally terminate a request and ~~and~~ , sends back a final response for that request ~~and reqests a default handling procedure~~ via the ISC interface to the S-CSCF, the S-CSCF shall abandon verification of the matching of the triggers of lower priority in the list~~perform the default handling treatment , i.e. discard the remaining list of filter criteria for that request~~. The final response shall include the indicator defined in step 3 b) i) above, so that the S-CSCF can correlate the messages.

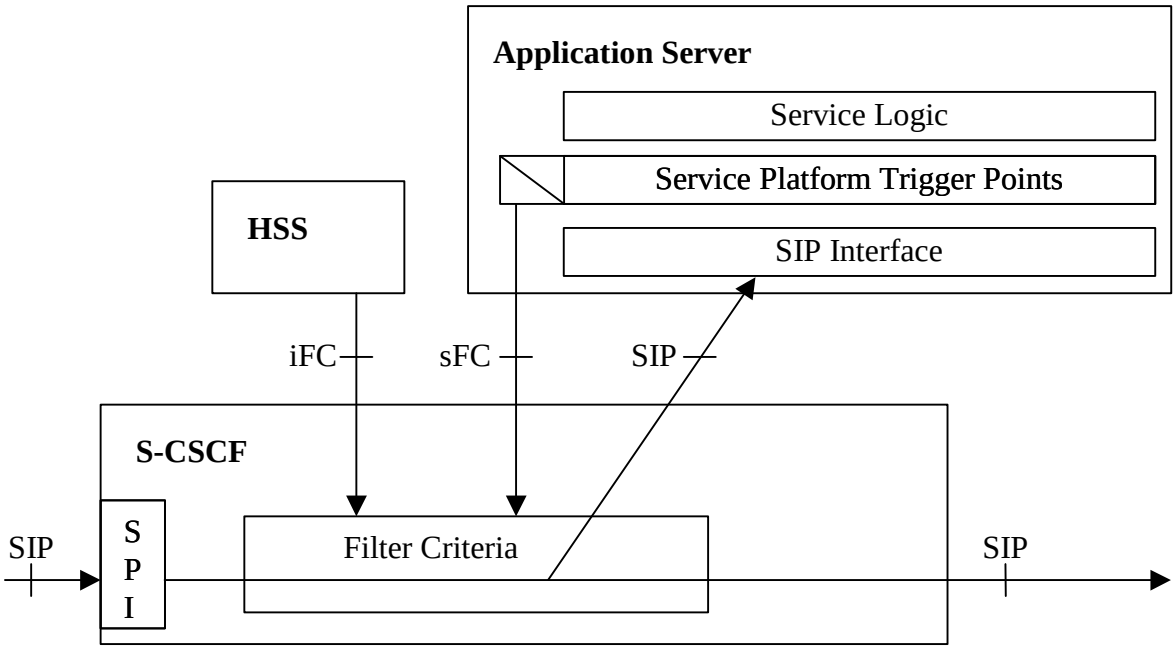

Figure 5.2.1: Application triggering architecture

Each invoked Application Server/service logic may decide not to be engaged with the invoked session by indicating that during the very first SIP transaction when the Record-Route/Route is generated for subsequent SIP requests. The denial shall mean that subsequent requests shall not be routed to such Application Servers/service logic any more during the lifetime of that session. Any Application Server, which has determined that it will not receive subsequent requests for a session cannot revoke this determination by means of Initial Filter Criteria (iFC).

Change

6.4 Handling of mobile originated IP multimedia sessions

The S-CSCF shall verify if the public user identity is barred. If so, it shall respond with a 4xx error code and stop further session processing.

The S-CSCF only looks for initial filter criteria when receiving an initial request ~~or refreshing request for a dialog...~~

The initial filter criteria (subset of the profile) has already been downloaded from the HSS and is stored locally at the S-CSCF, as specified in 3GPP TS 24.228 [4], and 3GPP TS 24.229 [5].

When such a session request comes in, the S-CSCF shall first check its triggers points (i.e., this is ~~an~~ a mobile originating request or a mobile terminating request). This clause describes the requirements for the S-CSCF when this request is ~~an~~ a mobile originating request. So ~~, if this request is an originating request,~~ the S-CSCF shall:

- check whether this request matches the initial filter criteria with the highest priority ~~of the application servers assigned~~ for that user by checking the service profile against the public user identity, which was used to place this request;

  if this 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;

- if this request does not match the highest priority initial filter criteria, check for matching of the following filter criteria priorities until one applies;

- if no more (or none) of the initial filter criteria apply, ~~of any application server,~~ the S-CSCF shall forward this request downstream based on the route decision;

- ~~if this request matches the initial filter criteria of only one application server and the S-CSCF has not interacted with that application server during this initial or refreshing transaction, the S-CSCF shall forward this request to that application server; if the S-CSCF has interacted with that application server in this transaction, the S-CSCF shall not forward this request to that application server but shall forward this request downstream based on the route decision;~~

- ~~if this originating request matches the initial filter criteria of more than one application server, the S-CSCF shall forward this request to the one which has not been interacted with in this transaction and has the highest priority according the Priority List given by HSS among those matched application servers; if all of them have been interacted in this transaction, the S-CSCF shall forward this request downstream based on the route decision; if the first attempt fails, the S-CSCF shall try others one by one according to their priories until there is a successful contact;~~

- in any instance, if the contact of the application server fails, the S-CSCF shall use the "default handling ~~treatment~~" associated with the ~~SPI~~initial Filter Criteria to determine if it shall either terminate the call, or let the call continue based on the information in the filter criteria; if the filter criteria doesn't contain instruction to the S-CSCF regarding the failure of the contact to the application server, the S-CSCF shall let the call continue as the default behaviour.

6.5 Handling of mobile terminated IP multimedia sessions

6.5.1 Handling of mobile terminated IP multimedia sessions, registered user

The S-CSCF shall verify if the public user identity is barred. If so, it shall respond with a 4xx error code and stop further session processing.

The S-CSCF only looks for initial filter criteria when receiving an initial request ~~or refreshing request for a dialog~~.

When such a request comes in, the S-CSCF shall first check this is an originating request or a terminating request. This clause describes the requirements for the S-CSCF when this request is a terminating request. So, if this request is a terminating request, the S-CSCF shall:

- if unavailable, download the relevant subscriber profile including the initial filter criteria from the HSS.
- use the initial Filter Criteria for the Mobile Termination;
  - ~~check whether this request matches the initial filter criteria of the application servers assigned for that user by checking the service profile against the public user identity, which this request was addressed to;~~
- the subsequent requirements for the S-CSCF are the same as those for handling originating sessions.

It may be possible that originating UE and terminating UE shares the same S-CSCF and AS, therefore the shared application server may interact with the S-CSCF twice in one transaction but in originating and terminating procedures respectively.

6.5.2 Handling of mobile terminated IP multimedia sessions, unregistered user

The S-CSCF shall verify if the public user identity is barred. If so, it shall respond with a 4xx error code and stop further session processing.

The S-CSCF only looks for initial filter criteria when receiving an initial request.

When such a request comes in, the S-CSCF shall first check this is an originating request or a terminating request. This clause describes the requirements for the S-CSCF when this request is a terminating request. So, if this request is a terminating request, the S-CSCF shall:

- if unavailable, download the relevant subscriber profile including the initial filter criteria from the HSS.
- use the initial Filter Criteria for the Mobile Termination for unregistered user;
- the subsequent requirements for the S-CSCF are the same as those for handling originating sessions.

It may be possible that originating UE and terminating UE shares the same S-CSCF and AS, therefore the shared application server may interact with the S-CSCF twice in one transaction but in originating and terminating procedures respectively.

Change

6.9 Description of subscriber data

6.9.1 Application Server subscription information

The Application Server Subscription Information is the set of all Filter Criteria that are stored within the HSS for service profile for a specific user. This information shall be sent by the HSS to the S-CSCF via the Cx Interface during registration.

6.9.2 Filter Criteria

This clause defines the contents of the Filter Criteria. This information is part of the Application Server Subscription Information. For further information about the XML modelling see 3GPP TS 29.228 [8].

Filtering is done for initial SIP request messages only.

The S-CSCF shall apply filter criteria to determine the need to forward SIP requests to Application Servers. These filter criteria will be downloaded from the HSS. ~~The HSS shall provide filter criteria in the prioritized list.~~

Initial Filter Criteria (iFC) are stored in the HSS as part of the user profile and are downloaded to the S-CSCF upon user registration, or upon a terminating initial request for an unregistered user if unavailable. They represent a provisioned subscription of a user to an application. After downloading the User Profile from the HSS, the S-CSCF assesses the filter criteria ~~activates for the indicated Application Server the Service Points of Interest that are correlated to the iFC in the User Profile~~. Initial Filter Criteria are valid throughout the registration lifetime of a user or until the User Profile is changed.

Subsequent Filter Criteria (sFC) are not used in this version of this specification.

6.9.2.1 Application Server address

Address to be used to access the Application Server for a particular subscriber.

6.9.2.2 Default ~~IP multimedia~~ handling ~~procedure~~

The Default ~~IP Multimedia H~~handling procedure indicates whether to abandon matching of lower priority triggers and to release the dialogue ~~IP Multimedia session shall be released~~; or to continue~~d~~ the dialogue and trigger matching. ~~as requested in case that AS requests to perform the default handling procedure during the dialogue between AS and S-CSCF or of loss of communications between the S-CSCF and Application Server is failed~~.

Use of the default handling procedure by the AS is not supported in this version of this specification.

6.9.2.3 Trigger point

Trigger Points are the information the S-CSCF receives from the HSS that defines the relevant SPIs for a particular application. They define the subset of initial SIP requests received by the S-CSCF that should be sent or proxied to a particular application. When the S-CSCF receives an initial SIP request, it evaluates the filter criteria one by one. If the initial SIP request matches the filter criteria, the S-CSCF proxies the SIP request to the corresponding SIP AS/IM-SSF/OSA SCS.

6.9.2.4 ~~Application Server priority list~~iFC Priority

If there are multiple ~~application servers~~initial Filter Criteria ~~are~~ assigned for one subscriber, ~~a~~ the priority shall ~~be assigned to application servers which~~ describes the order in which the S-CSCF shall assess them, and then contact the Application Servers ~~in case a~~when the SIP request matches the initial filter criteria ~~of more than one application server~~.

In this case, the S-CSCF shall interact with the application servers associated with the initial matching filter criteria, starting from the application server,filter criteria which has the highest priority.

6.9.2.5 Service Information

Service Information is an optional part of a Filter Criteria, which is a string of information. Service Information is transparent information, and is not processed by the HSS or the S-CSCF. Service Information is optionally part of an initial Filter Criteria. If it is available from the initial Filter Criteria the S-CSCF shall include it into the body of the SIP request which is sent from the S-CSCF to the AS to which the initial Filter Criteria is pointing to. Service Information is not processed, analysed or evaluated by the S-CSCF.

6.9.3 Authentication data

This clause defines the Authentication Data. This data shall be sent by the HSS to the S-CSCF via the Cx Interface during registration.

For definition of authentication data see specification 3GPP TS 23.008 [10]. For the handling of authentication data, see 3GPP TS 33.203 [11].

Change

7.2 Interfaces defined for HSS

7.2.1 HSS – CSCF (Cx) interface

This interface is used to send subscriber data to the S-CSCF, including Filter Criteria (and their priority); ~~to the S-CSCF; including Filter criteria,~~ which indicates which SIP requests should be proxied to which Application Servers.

The protocol used between the HSS and CSCF (Cx Interface) is specified in 3GPP TS 29.228 [8].

Change

B.3 Example information flows for a voicemail service

B.3.1 User out of coverage message recording

Figure B.3.1.1 shows a possible scenario of an Application Server, which acting as a terminating UA performs the function of a Voicemail Server in order to terminate a call and record a message on behalf of a UE that is out of coverage or powered off.

A S-CSCF is forwarded the initial INVITE destined for a UE that is not currently IMS registered. The Default Filter Criteria in the S-CSCF indicates that for the case of an unregistered user the INVITE should be forwarded to the Voicemail and Announcement Server.

Upon receiving the INVITE request the Voicemail and Announcement Server determines that the destination UE has subscribed to the Voicemail Service (possibly by downloading some subscriber profile information via the Sh interface). The Voicemail and Announcement Server therefore in addition to playing an announcement to inform the caller that the called party is either powered off or out of coverage also informs the caller that he may leave a message for the called party.

The calling party leaves a message for the called party and then hangs up the call by sending a BYE.

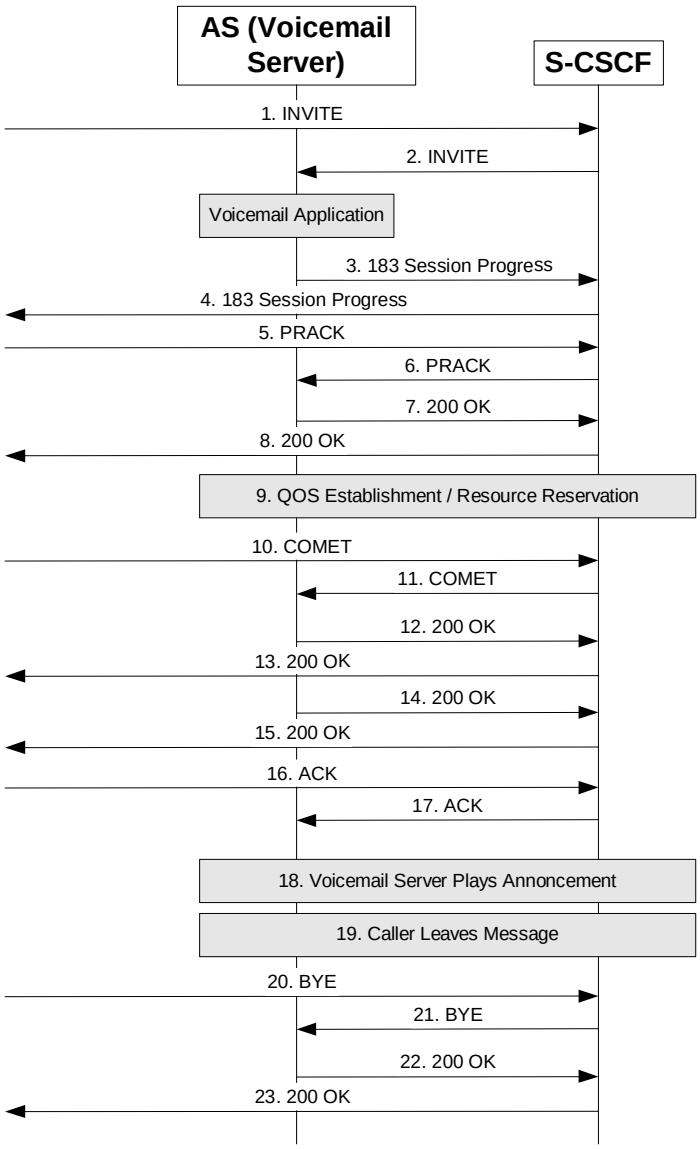

Figure B.3.1.1: Voicemail server records messages

Notes for figure B.3.1.1:

NOTE: For simplicity the 100 Trying response returned or received by the S-CSCF in reponse to requests is omitted from figure B.3.1.1.

1) INVITE request destined for an unregistered user is received at the S-CSCF ~~from caller~~.

2) Based on ~~Default~~ trigger point of the initial Filter Criteria S-CSCF proxies the INVITE request to the AS (Voicemail ~~and Announcement~~ Server) ~~(AS).~~

3-4) The AS starts the voicemail application and responds with a 183 Session Progress containing SDP which is proxied back to the caller by the S-CSCF.

5-8) The caller responds with a PRACK containing SDP, which the S-CSCF proxies to the AS and the AS responds with a 200 OK containing SDP which the S-CSCF proxies back to the caller.

QOS establishment and resource reservation takes place.

10-13) After completing resource reservation the caller sends a COMET containing SDP which is proxied by the S-CSCF to the AS which responds with a 200 OK containing SDP which is proxied back to the caller by the S-CSCF.

14-15) The AS then sends a 200 OK to the initial INVITE which the S-CSCF proxies to the caller.

16-17) The caller returns an ACK to the 200 OK.

18) The AS plays an announcement using the session established indicating that the caller is powered off but that the caller may leave a message.

19) The caller leaves a message using the session established.

20-21) The caller hangs up by sending a BYE which the S-CSCF proxies to the AS.

22-23) The AS responds with a 200 OK, which the S-CSCF proxies back to the caller.

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

Tdoc N1-021424

CR-Form-v5

CHANGE REQUEST

⌘ **23.218** **CR** **017** ⌘ **rev** **1** ⌘ Current version: **5.0.0** ⌘

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

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

Title:	⌘	Clarification to Handling of IP multimedia registration for barred public user identities
Source:	⌘	dynamicsoft
Work item code:	⌘	IMS-CCR
Date:	⌘	04.05.2002
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:	⌘	SA2 agreed that public user identities may be barred including temporary public user identities derived from a USIM.
Summary of change:	⌘	Clarification that the contents of the To header in the third party register request sent to an AS should be based on the public user identity in the filter criteria trigger.
Consequences if not approved:	⌘	Ambiguity in the specification regarding S-CSCF behaviour at registration regarding handling of Filter Criteria and barred public user identities.

Clauses affected:	⌘	6.3		
Other specs affected:	⌘	☒ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	24.229, 23.218 (CR XX), 23.228 (CR XX)
Other comments:	⌘			

6.3 Handling of IP multimedia registration

Upon receiving the initial registration request from the user, the S-CSCF shall authenticate the user and upon receiving a subsequent registration request containing valid authentication credentials, download the user profile from the HSS. For further detailed information on registration and authentication procedures see 3GPP TS 24.229 [5] and 3GPP TS 33.203 [11].

After a successfully authenticated registration, the S-CSCF shall download from the HSS all the implicitly registered public user identities associated with the registered public user identity and the S-CSCF shall then determine based on the filter criteria information downloaded from HSS which application servers to inform about the registration event of the public user identity(s). If the registration request matches the filter criteria of some application servers, the S-CSCF needs to inform the application servers by performing a third party registration to the those application servers which are interested to be informed about the user registration event of these public user identities.

The important information carried in the third party REGISTER request is the public user identity, the S-CSCF address and the expiration time. It shall be possible based on operator configuration to use one of the implicitly registered public user identities as the public user identity in the To: header of the third party REGISTER request sent to the Application Server. Additional application server specific data, which is associated with the Filter Criteria and obtained from the HSS, is added to the REGISTER request body. This data should include the IMSI for an Application Server that supports CAMEL services or the private user identity for other Application Servers as received from the HSS.

This third party registration will include an expiration time that is equal to the expiration time sent to the UE by the S-CSCF in the 200 OK response to the incoming REGISTER request

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

See figure 6.3.1:

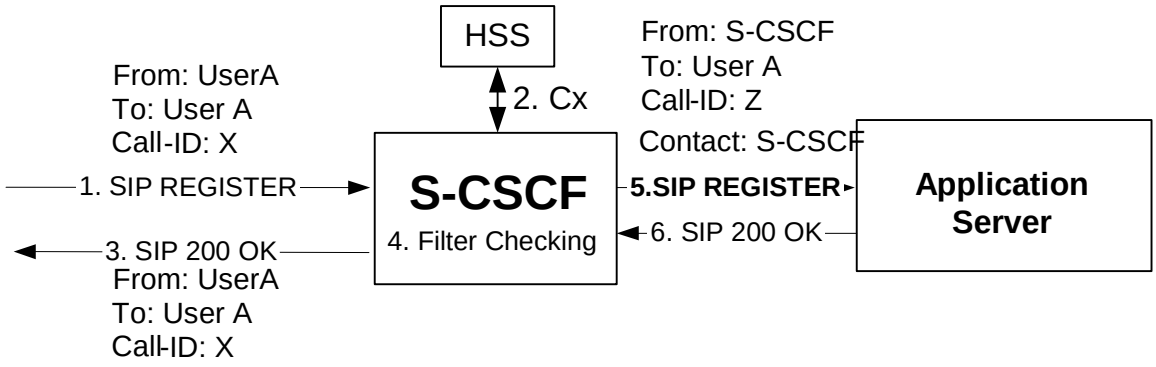

Figure 6.3.1: S-CSCF handling registration

Application Servers can in addition subscribe to the S-CSCF Registration Event Package. This provides a mechanism for the Application Server to discover all the implicitly registered public user identities without requiring multiple Register requests to be sent to the Application Server. The S-CSCF will send NOTIFY requests to the Application Server that has subscribed to the registration event package for the registered public user identity.

More information on these procedures is contained in 3GPP TS 24.229 [5].

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

Tdoc N1-021441

CR-Form-v5

CHANGE REQUEST

⌘ **24.229** **CR** **115** ⌘ **rev** **1** ⌘ Current version: **5.0.0** ⌘

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

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

Title:	⌘	Support for ISIM-less UICC
Source:	⌘	Ericsson, 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:	⌘	There is not support for UICCs that do not contain the ISIM application
Summary of change:	⌘	Addition of a pointer to 23.003 in the case the UICC does not contain the ISIM application. Clarification that the S-CSCF gets barred and non-barred implicitely public user identities from the HSS. Only the non-barred IDs are bound to the Contact. Clarification that the S-CSCF does not send the barred public user IDs in the NOTIFY. Addition of the S-CSCF barring an attempt to initiate or terminate a session with a barred public ID.
Consequences if not approved:	⌘	Only UICCs that contain the ISIM applicationwill work with IMS

Clauses affected:	⌘	3.2, 4.2, 5.1.1.,5.2.2, 5.4.2.1.2, 5.4.3.1, 5.4.3.2		
Other specs affected:	⌘	**X** Other core specifications	⌘	23.003, 24.228
		☐ Test specifications		
		☐ O&M Specifications		
Other comments:	⌘	Part of the functionality introduced by this CR is implemented in CR 060		

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

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

1xx	A status-code in the range 101 through 199, and excluding 100
2xx	A status-code in the range 200 through 299
AS	Application Server
AUTN	Authentication TokeN
BGCF	Breakout Gateway Control Function
c	conditional
CK	Ciphering Key
CN	Core Network
CSCF	Call Session Control Function
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
i	irrelevant
I-CSCF	Interrogating CSCF
IMSI	International Mobile Subscriber Identity
IK	Integrity Key
IM	IP Multimedia
IP	Internet Protocol
ISC	IP multimedia Subsystem Service Control
ISIM	IMS Suscriber Identity Module
m	mandatory
MAC	Message Authentication Code
MGCF	Media Gateway Control Function
MRFC	Media Resource Function Controller
n/a	not applicable
o	optional
P-CSCF	Proxy CSCF
PDU	Protocol Data Unit
RAND	RANDom challenge
RES	RESponse
RTP	Real-time Transport Protocol‘
S-CSCF	Serving CSCF
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SQN	SeQuence Number
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Universal Resource Identifier
USIM	UMTS Subscriber Identity Module
URL	Universal Resource Locator
x	prohibited

NEXT PROPOSED CHANGE

4.2 URL and address assignments

In order for SIP and SDP to operate, the following preconditions apply:

1) I-CSCFs used in registration are allocated FQDNs. Other IM CN subsystem entities may be allocated FQDNs. How these addresses are assigned to the logical entities is up to the network operator. For example, a single FQDN may be assigned to all I-CSCFs, and the load shared between various physical boxes by underlying IP capabilities, or a separate FQDN may be assigned to each I-CSCF, and the load shared between various physical boxes using DNS SRV capabilities.

Editor's note: The requirements for DNS-SRV entries or alternatives require further discussion.

2) All IM CN subsystem entities are allocated IP addresses. Allocation of IPv6 and IPv4 addresses fulfils the requirements of of 3GPP TS 23.221 [6] subclause 5.1.

3) The subscriber is allocated a private user identity by the home network operator, and this is contained within the ISIM application, if present, on the UICC. Where no ISIM application is present, the private user identity is derived from the IMSI, which is contained on the USIM (see 3GPP TS 23.003 [3]). This private user identity is available to the SIP application within the UE.

NOTE: The FQDNs may be resolved by using any of public DNSs, private DNSs, or peer-to-peer agreements.

4) The subscriber is allocated one or more public user identities by the home network operator. At least one of these is contained within the ~~USIM~~ISIM application, if present, on the UICC. Where no ISIM application is present, the UE shall derive a temporary public user identity from the IMSI contained on the USIM (see 3GPP TS 23.003 [3]). All registered public user identities are available to the SIP application within the UE, after registration.

5) The UE is dynamically assigned an IP version 6 address.

NEXT PROPOSED CHANGE

5 Application usage of SIP

5.1 Procedures at the UE

5.1.1 Registration and authentication

5.1.1.1 General

The UE shall register public user identities (see table A.3/1 and dependencies on that major capability).

In case a UE registers several public user identities at different points in time, the procedures to re-register, deregister and subscribe to the registration-state event package for these public user identities can remain uncoordinated in time.

5.1.1.1A Parameters contained in the UICC

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

- the private user identity;
- one ore more public user identities; and
- the home network domain name used to address the SIP REGISTER request

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

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to.

All these three parameters are derived from the IMSI parameter in the USIM, according to the procedures described in 3GPP TS 23.003 [3].

The temporary public user identity is only used in REGISTER requests. After a successful registration, the UE will get the associated public user identities, and any of them shall be used in subsequent non-REGISTER messages.

As the temporary public user identity may be barred, the UE shall not ~~indicate~~reveal ~~to the user~~ the temporary public user identity to the user.

In the case the UE needs to derive the temporary public user identity, the procedure shall be executed every time the UICC is changed.

5.1.1.2 Initial registration

The UE can register a public user identity at any time that a valid PDP context exists.

A REGISTER request may be integrity protected using IK, see 3GPP TS 33.203 [14], received in an earlier registration.

The public user identity to be registered can be extracted either from the ISIM application, if present, on the UICC~~SIM~~ or derived from the USIM, according to the procedures described in subclause 5.1.1.1A. ~~If no ISIM is present, the UE shall use the temporary public user identity derived the temporary public user identity from the IMSI contained on the~~

~~USIM.~~ ~~or~~ A public user identity may be input ~~from~~ by the end user. On sending a REGISTER request, the UE shall populate the header fields as follows:

a) the user ID field of the authentication protocol, carried in the Authorization header, shall contain the private user identity~~. This shall be extracted from the ISIM application, if present, contained on the UICC. If no ISIM application is present, the private user identity id derived from shall be extracted from the IMSI contained on the USIM (see 3GPP TS 23.003[3])~~;

b) the From header shall contain ~~the temporary public user identity, derived from the IMSI contained on the USIM (see 3GPP TS 23.003 [3]) or shall contain~~ the public user identity to be registered;

c) the To header shall contain ~~the temporary public user identity, derived from the IMSI contained on the USIM (see 3GPP TS 23.003 [3]) or shall contain~~ the public user identity to be registered;

d) the Expires header, or the expires parameter within the Contact header, shall contain 600 000 seconds as the value desired for the duration of the registration;~~.~~

e) a Request-URI that contains the SIP URI of the domain name of the home network.

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

The UE shall extract or derive from the UICC a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A.

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

On receiving the 200 OK response to the REGISTER request, the UE shall store the expiration time of the registration.

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

On receiving a 423 Registration too brief response to the REGISTER request, the UE shall:

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

5.1.1.3 Initial subscription to the registration-state event package

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the users registration-state event package for the public user identity registered as described in subclause 5.1.1.2 at the users registrar (S-CSCF). Therefore the UE shall generate a SUBSCRIBE request with the following elements:

- a Request URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URL that contains ~~the~~ a public user identity ~~that was previously registered~~;
- a From header set to a SIP URL that contains ~~the~~ a public user identity ~~that was previously registered~~;
- a To header, set to a SIP URL that contains ~~the~~ a public user identity ~~that was previously registered~~;
- an Event header set to the "registration-state" event package;
- an Expires header set to a value higher than the Expires header of the before sent REGISTER request.

Afterwards it shall send out the so generated SUBSCRIBE request.

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

The UE shall automatically resubscribe to the registration-state event package for a previously registered public user identity if the expiration time, as indicated in the Expires header of the 2xx response to the SUBSCRIBE message, has run out and the public user identity is still registered.

NEXT PROPOSED CHANGE

5.2 Procedures at the P-CSCF

5.2.1 General

The P-CSCF shall support use of the Path header.

NOTE: The Path header is only applicable to the REGISTER request and its 200 OK response.

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.

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.

NEXT PROPOSED CHANGE

5.4.2.1.2 Notification about registration state

Notification of the registration state shall affects the non-barred public user identities. The barred public user identities ~~are~~shall never be sent in a NOTIFY message.

If the registration state of one or more non-barred public user identities changes, the S-CSCF shall generate a NOTIFY request on all dialogs which have been established due to subscription to the registration-state event package of that user. For each NOTIFY request, the S-CSCF shall:

- set the Request-URI and Route header to the saved route information during subscription;
- set the Event header to the "registration-state" value;
- indicate registration state "open" for all public user identities which are currently registered;
- indicate registration state "closed" for all public user identities which are currently deregistered; and
- indicate within the "<detail>" information of those public user identities which will be automatically reregistered the "automatically by" information, followed by the specific public user identity which will cover the reregistration.

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

```
<tuple name="sip:user1_public1@home1.net">
  <status><value>open</value></status>
</tuple>

<tuple name="sip:user1_public2@home1.net">
  <status> <value>open</value> </status>
  <detail>automatically by sip:user1_public1@home1.net</detail>
</tuple>
```

Afterwards the S-CSCF shall send the generated NOTIFY request on the dialog and await a 2xx response.

NEXT PROPOSED CHANGE

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:

- determine whether the request contains a barred public user identity in the From or Remote-Party-ID header fields of the request or not. In case any of the said header fields contains a barred public user identity for the user, then the S-CSCF shall reject the request by generating a 403 (Forbidden) response. Otherwise, continue with the rest of the steps.

- remove its own SIP URL from the topmost Route header;

- if the outgoing Request-URI is a TEL URL, the S-CSCF shall translate the E.164 address (see RFC 2806 [16]) to a globally routable SIP URL using an ENUM/DNS translation mechanism with the format specified in RFC 2916 [18]. Databases aspects of ENUM are outside the scope of the present document. If this translation fails, the request may be forwarded to a BGCF or any other appropriate entity (e.g a MRFC to play an announcement) in the originator's home network or an appropriate SIP response shall be sent to the originator;

- check if <original-dialog-id> XML element is present in the payload of the incoming request. If present, it indicates an association with an existing dialog, the request has been sent from an Application Server in response to a previously sent request. The <od-to>, <od-from> and <od-call-id> XML element values from the <original-dialog-id> XML element may be used as additional parameters when searching for existing dialogs. Local data shall be updated to indicate that this Application Server has been contacted for the initial request. The S-CSCF shall determine the next hop using initial filter criteria and local data on status of which Application Servers have been contacted. If the next hop is another Application Server, the S-CSCF shall retain the <original-dialog-id> XML element in the message body of the request. If the next hop is not an Application Server, the S-CSCF shall leave out the <original-dialog-id> XML element from the payload of the request;

- check whether the initial request matches the initial filter criteria of the application servers assigned for the public user identity as described in 3GPP TS 23.218 [5] subclause 6.4. Depending on the result of the previous check, the S-CSCF may contact one or more application server(s) before processing the outgoing Request-URI. In case of contacting one or more application server(s) the S-CSCF shall:

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

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

- store the value of the <icid> XML element received in the message body (see subclause 7.6) and retain the <icid> XML element in the message body;

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

- in case of an initial request for a dialog the S-CSCF shall create a Record-Route header containing its own SIP URL and save the necessary header fields from the request (and from its appropriate responses) in order to release the dialog when needed.

When the S-CSCF receives from the served 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.

NEXT PROPOSED CHANGE

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.

When the S-CSCF receives a request destined for a barred public user identity, the S-CSCF shall return an appropriate unsuccessful SIP response. This response may be, e.g., a 404 (Not found) or 604 (Does not exist anywhere).