Source: **TSG SA WG2**
Title: **CRs on 23.228 (IMS Stage 2)**
Agenda Item: **7.2.3**

The following Change Requests (CRs) have been approved by TSG SA WG2 and are requested to be approved by TSG SA plenary #23.
Note: the source of all these CRs is now S2, even if the name of the originating company(ies) is still reflected on the cover page of all the attached CRs.

S2 doc #	Title	Spec	CR #	cat	Version in	REL	WI	S2 meeting	Clauses affected
S2-040828	Relation of IMS sessions and PDP Contexts	23.228	**410**	F	5.11.0	5	IMS-CCR	S2 #38	4.2.5.1
S2-040974	Relation of IMS sessions and PDP Contexts	23.228	**395r5**	B	6.4.1	6	IMS2	S2 #38	E.2.2.1
S2-040936	Session based messaging: general principles	23.228	**381r3**	B	6.4.1	6	IMS2	S2 #38	2, 5.16.2.1, 5.16.2.2
S2-040382	Session based Messaging without preconditions	23.228	**382r1**	B	6.4.1	6	IMS2	S2 #37	5.16.2.2.1
S2-040435	Session based Messaging with AS intermediate node	23.228	**384r2**	B	6.4.1	6	IMS2	S2 #37	New Clause 5.16.2.2.3
S2-040940	Session based messaging release procedure	23.228	**385r2**	B	6.4.1	6	IMS2	S2 #38	5.16.2.2.4 (new)
S2-040968	An optimisation in registration information flow for user not registered	23.228	**387r2**	F	6.4.1	6	IMS2	S2 #38	5.2.2.3, 5.2.2.4, 5.12.1
S2-040387	Registration and Public User Identity	23.228	**390r1**	F	6.4.1	6	IMS2	S2 #37	5.2.1, 5.2.1a
S2-040954	Record Route at S-CSCF	23.228	**391r5**	B	6.4.1	6	IMS2	S2 #38	5.4.5, new informative annex F
S2-040398	Alignment of headings with drafting rules	23.228	**393r1**	D	6.4.1	6	IMS2	S2 #37	3.3, 4.0, 4.2.5.1, 4.3.3.0, 4.6.0, 4.6.2.0, 4.10.0, 5.0, 5.1.1.0, 5.1.5.0, 5.2.0, 5.2.1a.0, 5.3.2.0, 5.3.2.2.0, 5.4.0, 5.4.6.0, 5.4.7.0, 5.4.9.0, 5.4.12.0, 5.5.0, 5.6.0, 5.7.0, 5.8.0, 5.10.0, 5.10.3.1.0, 5.11.1.0, 5.11.2.0, 5.11.3.0, 5.11.4.0, 5.11.5.0, 5.11.6.0, 5.11.6.2.0, 5.12.0, 5.13.0, 5.14.0, 5.15.0, 5.16.0, 5.16.1.0, 5.16.1.1.0, 5.16.2.0, 5.16.2.2.0, 5.18.0, E.0, E.1.0, E.1.1.0, E.2.1.0, E.2.2.0, E.2.3.0, and E.2.4.0
S2-040440	PSI clean-up	23.228	**394r2**	F	6.4.1	6	IMS2	S2 #37	5.4.12.1, 5.4.12.2, 5.4.12.3, 5.4.12.4
S2-040401	Support for Caller preferences	23.228	**396r1**	B	6.4.1	6	IMS2	S2 #37	2, 4.2.7.3, 4.6.3
S2-040937	Message size limitations for	23.228	**397r3**	C	6.4.1	6	IMS2	S2 #38	2, 5.16.1.1

	Immediate messaging								
S2-040938	Session based messaging requirements and flows	23.228	**398r4**	B	6.4.1	6	IMS2	S2 #38	5.16.2.2.2
S2-040403	Reference to Local Services in Chapter 4.3.3.3a of 23.228	23.228	**399r1**	D	6.4.1	6	IMS2	S2 #37	4.3.3.3a
S2-040942	Proposed clarifications to MRFC/MRFP	23.228	**403r1**	C	6.4.1	6	IMS2	S2 #38	4.7
S2-040943	Relationship between private user IDs and IMS subscription	23.228	**404r1**	F	6.4.1	6	IMS2	S2 #38	4.3.3.4, 4.7, and 5.2.1a
S2-040952	Resource reservation in IMS	23.228	**405r1**	C	6.4.1	6	IMS2	S2 #38	4.2.5, 5.4.8
S2-040953	Architectural support for AS origination	23.228	**406r1**	C	6.4.1	6	IMS2	S2 #38	4.6.3, 5.3.1, 5.3.2.1, new section 5.6.5
S2-041021	Clarification of forking capabilities	23.228	**407r2**	C	6.4.1	6	IMS2	S2 #38	4.2.7.2
S2-040969	PSIs for local services	23.228	**408r1**	F	6.4.1	6	IMS2	S2 #38	4.2.2
S2-041022	Group management clarification	23.228	**409r2**	C	6.4.1	6	IMS2	S2 #38	3.3, 4.10.1

3GPP TSG SA WG2 meeting #38
Atlanta, USA, 16th – 20th February 2004

Tdoc ⌘S2-040936

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **381** ⌘ **rev** **3** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Session based messaging: general principles
Source:	⌘	SA2 (Nokia, Ericsson, RIM, Siemens, Lucent)
Work item code:	⌘	IMS2
Date:	⌘	16/02/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	S2-033769 introduced some architectural principles for messaging sessions this CR adds additional principles.
Summary of change:	⌘	The CR provides guidance as to the use of preconditions with session based messaging and also clarifies that the UE needs to indicate the ability to host the message session.
Consequences if not approved:	⌘	Stage 2 work on session based messaging is not complete.

Clauses affected:	⌘	2, 5.16.2.1, 5.16.2.2			
		Y	**N**		
Other specs Affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

<< First Changed section >>

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 TS 23.002: "Network Architecture".

[2] CCITT Recommendation E.164: "Numbering plan for the ISDN era".

[3] CCITT Recommendation Q.65: "Methodology – Stage 2 of the method for the characterisation of services supported by an ISDN".

[4] ITU Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN"

[5] GSM 03.64: "Digital cellular telecommunication system (Phase 2+); Overall Description of the General Packet Radio Service (GPRS) Radio Interface; Stage 2".

[6] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[7] 3GPP TS 23.221: "Architectural Requirements".

[8] 3GPP TS 22.228: "Service requirements for the IP multimedia core network subsystem"

[9] 3GPP TS 23.207: "End-to-end QoS concept and architecture"

[10] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP"

[10a] 3GPP TS 24.229: " IP Multimedia Call Control based on SIP and SDP; Stage 3"

[11] 3GPP TS 25.301: "Radio interface protocol architecture"

[11a] 3GPP TS 29.207: " Policy control over Go interface "

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

[13] RFC 2396: "Uniform Resource Identifiers (URI): Generic Syntax"

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

[15] RFC 2806: "URLs for Telephone Calls"

[16] RFC 2916: "E.164 number and DNS"

[16a] RFC 3041: "Privacy Extensions for Stateless Address Autoconfiguration in IPv6"

[17] ITU Recommendation G.711: "Pulse code modulation (PCM) of voice frequencies"

[18] ITU Recommendation H.248: "Gateway control protocol"

[19] 3GPP TS 33.203: "Access Security for IP-based services"

[20] 3GPP TS 33.210: "Network Domain Security: IP network layer security "

[21] 3GPP TS 26.235: "Packet Switched Multimedia Applications; Default Codecs".

[22] 3GPP TR 22.941: " IP Based Multimedia Services Framework "

[23] 3GPP TS 23.060: “General Packet Radio Service (GPRS); Service description; Stage 2

[24] 3GPP TS 23.003: “Technical Specification Group Core Network; Numbering, addressing and identification”

[25] 3GPP TS 32.200: “Telecommunication management; Charging management; Charging principles”

[26] 3GPP TS 32.225: ” Telecommunication Management; Charging Management; Charging Data Description for IP Multimedia Subsystem”

[27] 3GPP TS 22.071: “Technical Specification Group Services and System Aspects,Location Services (LCS);Service description, Stage 1”

[28] 3GPP TS 23.271: “Technical Specification Group Services and System Aspects, Functional stage 2 description of LCS”

[29] 3GPP TS 23.078: “Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 3 - Stage 2”

[29a] 3GPP TS 22.340: “ IMS Messaging; Stage 1”

[30] 3GPP TS 29.228:“IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents”

[31] 3GPP TS 23.240: "3GPP Generic User Profile - Architecture; Stage 2"

[32] 3GPP TS 22.250: “IP Multimedia Subsystem (IMS) group management”; Stage 1”

[33] RFC 2766: “Network Address Translation-Protocol Translation (NAT-PT)”

[34] RFC 2663: “IP Network Address Translator (NAT) Terminology and Considerations”

[35] Transition Scenarios for 3GPP Networks, draft-ietf-v6ops-3gpp-cases-03.txt, work in progress

[36] 3GPP TS 23.141: “Technical Specification Group Services and System Aspects, Presence Service”

[37] 3GPP TS 26.xxx:” IMS messaging and Presence; Media formats and codecs”

[38] draft-ietf-sip-callee-caps-01 (October 2003): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"

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

[39] IETF RFC 3323 (2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[40] IETF RFC 3325 (2002): "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Network".

[41] RFC 3312 (October 2002): "Integration of resource management and Session Initiation Protocol (SIP)".

<< Second Changed section >>

5.16.2 Session-based Messaging

This subclause describes architectural concepts and procedures for fulfiling the requirements for Session-based Messaging described in TS 22.340 [29a].

5.16.2.1 Architectural principles

Session-based IMS messaging communications shall as much as possible use the same basic IMS session delivery mechanisms (e.g. routing, security, service control) as defined in clause 4 and 5 of this document. For session based messaging the session shall include a messaging media component, other media components may also be included.

When the messaging media component does not require QoS beyond best-effort, it is expected that the UE will have an appropriate IP-CAN bearer available for the messaging media component prior to starting session initiation. In the case when the messaging media component does not require the reservation of additional bearer resources, the UE shall not require the use of the preconditions mechanism defined in RFC 3312[41] for Session based messaging establishment.

Once the session containing a messaging media component is established, messages in the session are transported between the session participants as per the parameters defined in the messaging media component part of the session description (SDP).

In the SDP offer the UE should offer to host the message session (accept a connection for the message session from the other endpoint) and indicate that it is also prepared for the other party to host the message session. In order to offer to host the message session the UE first needs an IP-CAN bearer on which it can accept the connection for the message media component.

NOTE: SBLP applied to session-based messaging media components restricts the ability of the UE to host the message session.

Messages within a message session should be transported over a connection-oriented reliable transport protocol. Message sessions may be either established end to end between two UEs or may involve one or more intermediate nodes (e.g. a chat server for multi party chat or to perform per message charging).

For addressing chat-group-type session based messaging the concept of Public Service Identities is used.

Session based messaging is available for users that are registered in the IMS.

The session based messaging shall be able to provide the following functionality:

-Per-message-based charging, as well as content- and size-based charging.

-Operator-controlled policy to be set on the size and content of the messages.

-Support for a messaging media component as part of a session where other media components are also included.

-Support for messaging-only sessions.

5.16.2.2 Procedures to enable Session based Messaging

IMS users shall be able to exchange session-based messages with each other by using the procedures described in this sub-clause. These~~This~~ procedures shall allow the exchange of any type of multimedia content (subject to possible restrictions based on operator policy and user preferences/intent), for example but not limited to:

- Pictures, video clips, sound clips with a format defined by 3GPP TS 26.xxx [37]

5.16.2.2.1 Session based messaging procedure to registered public user identity

Editor's note: This sub-clause will describe session based messaging between two UEs.

5.16.2.2.2 Session based messaging procedure using multiple UEs

Editor's note: This sub-clause will describe session based messaging between multiple UEs using for example a Chat session.

3GPP TSG SA WG2 meeting #37
Innsbruck, Austria, 12th – 16th January 2004

Tdoc ⌘S2-040382

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** 382 ⌘ **rev** **1** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Session based messaging without preconditions
Source:	⌘	SA2 (RIM)
Work item code:	⌘	IMS2
Date:	⌘	15/01/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	S2-033769 introduced some architectural principles for messaging sessions.
Summary of change:	⌘	The CR introduces flows and procedures, which show the of a message session where the messages are exchanged e2e between the two endpoints.
Consequences if not approved:	⌘	Stage 2 work on session based messaging is not complete.

Clauses affected:	⌘	5.16.2.2.1			
Other specs Affected:	⌘	Y	N		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

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

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

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

<< Changed section >>

5.16.2 Session-based Messaging

This subclause describes architectural concepts and procedures for fulfiling the requirements for Session-based Messaging described in TS 22.340 [29a].

5.16.2.1 Architectural principles

Session-based IMS messaging communications shall as much as possible use the same basic IMS session delivery mechanisms (e.g. routing, security, service control) as defined in clause 4 and 5 of this document. For session based messaging the session shall include a messaging media component, other media components may also be included. Once the session containing a messaging media component is established, messages in the session are transported between the session participants as per the parameters defined in the messaging media component part of the session description (SDP).

For addressing chat-group-type session based messaging the concept of Public Service Identities is used.

Session based messaging is available for users that are registered in the IMS.

The session based messaging shall be able to provide the following functionality:

-Per-message-based charging, as well as content- and size-based charging.

-Operator-controlled policy to be set on the size and content of the messages.

-Support for a messaging media component as part of a session where other media components are also included.

-Support for messaging-only sessions.

5.16.2.2 Procedures to enable Session based Messaging

IMS users shall be able to exchange session-based messages with each other by using the procedure described in this sub-clause. This procedure shall allow the exchange of any type of multimedia content (subject to possible restrictions based on operator policy and user preferences/intent), for example but not limited to:

- Pictures, video clips, sound clips with a format defined by 3GPP TS 26.xxx [37]

5.16.2.2.1 Session based messaging procedure to registered public user identity

~~Editor's note: This sub-clause will describe session based messaging between two UEs.~~

The following procedure shows the establishment of a message session between two registered UEs where the UEs are able to exchange messages end-to-end.

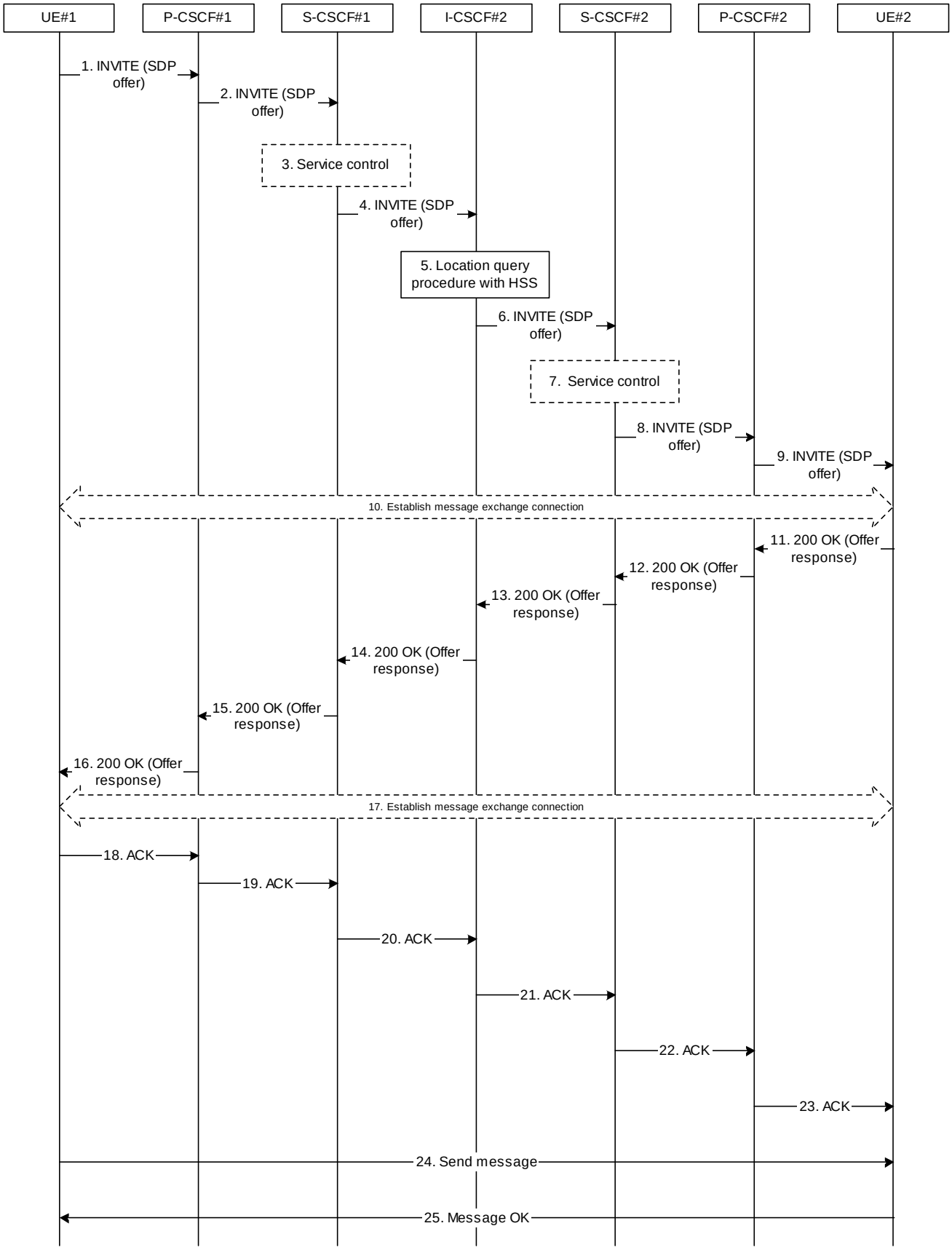


Figure X.1: Message session establishment

1. UE#1 sends the SIP INVITE request, containing an initial SDP, to the P-CSCF. The initial SDP indicates that UE#1 wishes to establish a message session and whether the UE#1 is able to host the session.

2. P-CSCF#1 forwards the INVITE request to S-CSCF#1 along the path determined upon UE#1's most recent registration procedure.

3. Based on operator policy S-CSCF#1 may reject the INVITE request with an appropriate response. S-CSCF#1 may invoke whatever service control logic is appropriate for this INVITE request. This may include routing the INVITE request to an application server, which processes the request further on.

4. S-CSCF#1 forwards INVITE request to I-CSCF#2.

5. I-CSCF#2 performs Location Query procedure with the HSS to acquire the S-CSCF address of the destination user (S-CSCF#2).

6. I-CSCF#2 forwards INVITE request to S-CSCF#2.

7. Based on operator policy S-CSCF#2 may reject the INVITE request with an appropriate response. S-CSCF#2 may invoke whatever service control logic is appropriate for this INVITE request. This may include routing the INVITE request to an application server, which processes the request further on.

8. S-CSCF#2 forwards the INVITE request to P-CSCF#2 along the path determined upon UE#2's most recent registration procedure.

9. P-CSCF#2 forwards the INVITE request to UE#2.

10. If UE#1 offered to host the session then UE#2 establishes with UE#1 a reliable end-end connection for exchange of the message media.

11. – 16. UE#2 accepts the message session with a 200 OKresponse.The 200 OK response traverses back to UE#1.

17. If UE#1 requested UE#2 to host the session then UE#1 establishes with UE#2 a reliable end-end connection for exchange of the message media.

18-22. UE#1 acknowledges the 200 OK with an ACK which traverses back to UE#2.

24. UE#1 generates the message content and sends it to UE#2 using the established message connection.

25. UE#2 acknowledges the message with a response that indicates that the UE#2 has received the message. The response traverses back to UE#1. After receiving the message UE#2 renders the multimedia content to the user.

Further messages may be exchanged in either direction between UE#1 and UE#2 using the established connection.

5.16.2.2.2 Session based messaging procedure using multiple UEs

Editor's note: This sub-clause will describe session based messaging between multiple UEs using for example a Chat session.

3GPP TSG SA WG2 meeting #37
Innsbruck, Austria, 12th – 16th January 2004

Tdoc ⌘S2-040435

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** 384 ⌘ **rev** **2** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Session based messaging with AS intermediate node
Source:	⌘	SA2 (RIM)
Work item code:	⌘	IMS2
Date:	⌘	15/01/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	S2-033769 introduced some architectural principles for messaging sessions.
Summary of change:	⌘	The CR introduces flows and procedures, which show the establishment of a message session where the messages are exchanged via an intermeadiate node (e.g performing per message charging).
Consequences if not approved:	⌘	Stage 2 work on session based messaging is not complete.

Clauses affected:	⌘	New Clause 5.16.2.2.3			
Other specs Affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

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

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

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

<< Changed section >>

5.16.2 Session-based Messaging

This subclause describes architectural concepts and procedures for fulfiling the requirements for Session-based Messaging described in TS 22.340 [29a].

5.16.2.1 Architectural principles

Session-based IMS messaging communications shall as much as possible use the same basic IMS session delivery mechanisms (e.g. routing, security, service control) as defined in clause 4 and 5 of this document. For session based messaging the session shall include a messaging media component, other media components may also be included. Once the session containing a messaging media component is established, messages in the session are transported between the session participants as per the parameters defined in the messaging media component part of the session description (SDP).

For addressing chat-group-type session based messaging the concept of Public Service Identities is used.

Session based messaging is available for users that are registered in the IMS.

The session based messaging shall be able to provide the following functionality:

-Per-message-based charging, as well as content- and size-based charging.

-Operator-controlled policy to be set on the size and content of the messages.

-Support for a messaging media component as part of a session where other media components are also included.

-Support for messaging-only sessions.

5.16.2.2 Procedures to enable Session based Messaging

IMS users shall be able to exchange session-based messages with each other by using the procedure described in this sub-clause. This procedure shall allow the exchange of any type of multimedia content (subject to possible restrictions based on operator policy and user preferences/intent), for example but not limited to:

- Pictures, video clips, sound clips with a format defined by 3GPP TS 26.xxx [37]

5.16.2.2.1 Session based messaging procedure to registered public user identity

Editor's note: This sub-clause will describe session based messaging between two UEs.

5.16.2.2.2 Session based messaging procedure using multiple UEs

Editor's note: This sub-clause will describe session based messaging between multiple UEs using for example a Chat session.

5.16.2.2.3 Session based messaging procedure with an intermediate node

The following procedure shows the originating session based messaging involving an intermediate node.

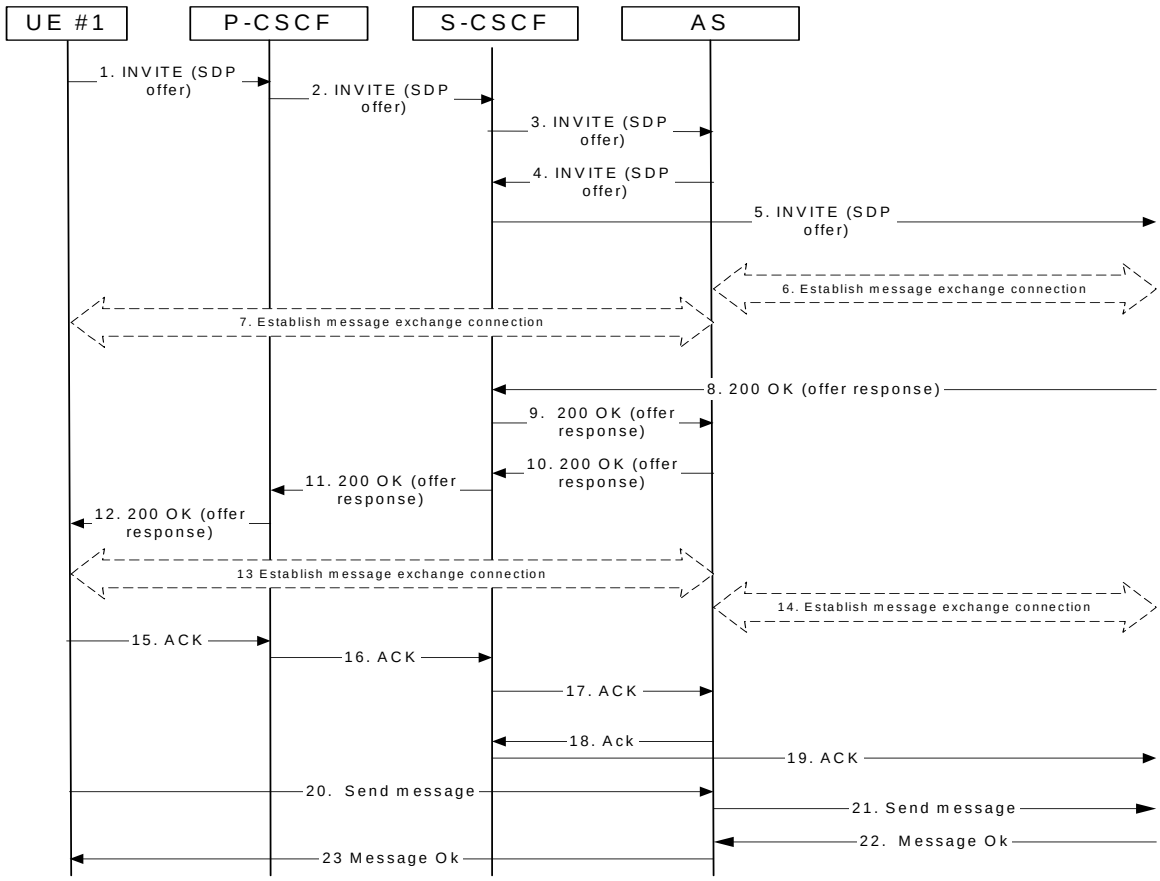


Figure X.3: Session based messaging with an intermediate node

1. UE#1 sends the SIP INVITE request addressed to UE#2, containing an initial SDP, to the P-CSCF. The initial SDP indicates that UE#1 wishes to establish a message session and whether the UE#1 is able to host the session.

2. P-CSCF#1 forwards the INVITE request to S-CSCF along the path determined upon UE#1's most recent registration procedure.

3. Based on operator policy S-CSCF may reject the INVITE request with an appropriate response. S-CSCF may invoke whatever service control logic is appropriate for this INVITE request. In this case the Filter Criteria trigger the INVITE request to be routed to an application server that acts as as an intermediate node for the message session.

4. The AS may modify the contents of the SDP (such as IP address/port numbers). The AS sends the INVITE request to S-CSCF

5. S-CSCF forwards the INVITE request to the destination network. The destination network will perform the terminating procedure.

6. If UE#1 offered to host the session then the destination UE or AS in the terminating network establishes with the AS a reliable end-end connection for exchange of the message media.

7. If UE#1 offered to host the session then the AS establishes with UE#1 a reliable end-end connection for exchange of the message media.

8. – 9. The UE or AS in the terminating network accepts the message session with a 200 OKresponse.The 200 OK response is forwarded to the AS by the S-CSCF

10. – 12. The AS accepts the message session with a 200 OKresponse.The 200 OK response traverses back to UE#1

13. If UE#1 requested the other party to host the session then UE#2 establishes with the AS a reliable end-end connection for exchange of the message media.

14. If UE#1 requested the other party to host the session then the AS establishes with the UE or AS in the terminating network a reliable end-end connection for exchange of the message media.

15-17. UE#1 acknowledges the 200 OK with an ACK which traverses back to the AS.

18-19. The AS acknowledges the 200 OK response by an ACK from UE#1 which traverses back to the UE or AS in the terminating network via the S-CSCF.

20. UE#1 generates the message content and sends it to the AS using the established message connection.

21. The AS forwards the message content and using the established message connection with the terminating network.

22. The UE or AS in the terminating network acknowledges the message with a response that indicates that the reception of the message. The response traverses back to the AS.

23. The AS forwards the response that back to UE#1.

Further messages may be exchanged in either direction between UE#1 and the terminating network using the established connection via the AS.

3GPP TSG-SA WG2 Meeting #38
Atlanta, USA, 16th – 20th February 2004

Tdoc ⌘S2-040940

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **385** ⌘ **rev** **2** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Session based messaging release procedure
Source:	⌘	SA2 (RIM, Siemens)
Work item code:	⌘	IMS2
Date:	⌘	18/02/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	S2-033769 introduced some architectural principles for messaging sessions. Basic messaging principles were agreed at SA2#37, but there was no final agreeement on the release procedure. Concerns were expressed that the signalling connection is released before the actual message connection is destroyed. However, there is no other way for the UE to indicate its intention to end a message session by sending a SIP BYE request to the other party. Thus, it is straightforward that the actual TCP connection is teared down after the other party has agreed to stop the session.
Summary of change:	⌘	The CR introduces flows and procedures, which show the release of a message session. Introduces release procedure for message session according the IETF messaging draft. It is proposed that the session host shall destroy the local session state and tear down the TCP connection after receiving the acknowledgement from the other party. Otherwise lost of the TCP connection may be interpreted as a failure condition.
Consequences if not approved:	⌘	Stage 2 work on session based messaging is not complete.

Clauses affected:	⌘	5.16.2.2.4 (new)

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

Other comments: ⌘	

How to create CRs using this form:

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

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

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

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

********** First Change**********

5.16.2.2.4 Session based messaging release procedure

The following procedure shows the release of a message session, which was established between two UEs. It is assumed that UE#1 is the session host.

Note 1: The following call flow may be not applicable in case SBLP is used.

Note 2: The following call flow assumes that a separate IP-CAN bearer is used to send and receive messages.

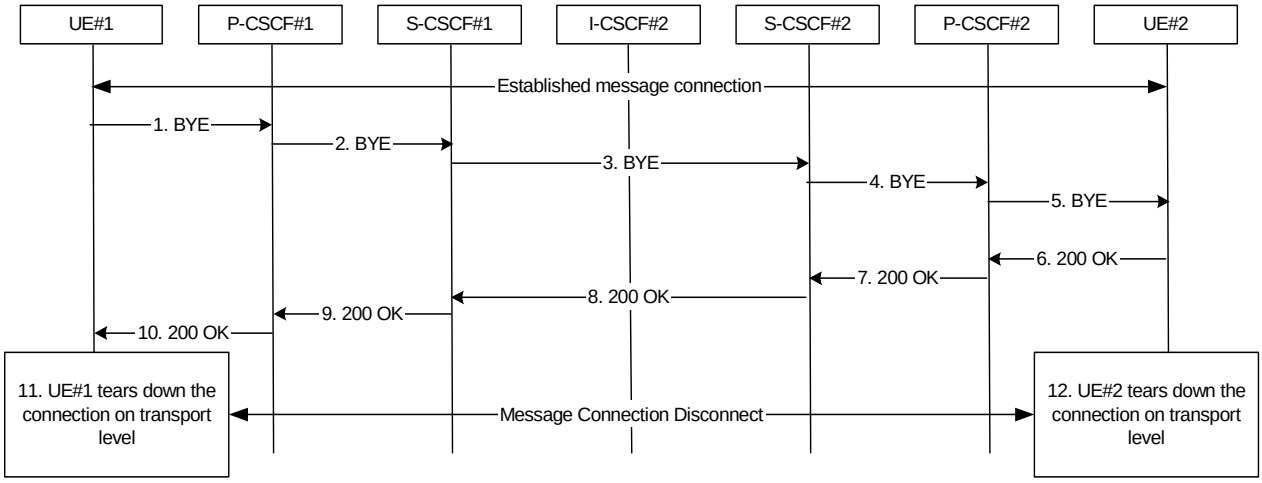


Figure X: Message session release procedure

1. – 5. UE#1 indicates its intent to terminate the message session by sending a BYE request to UE#2.

6. – 10. UE#2 agrees to end the session and acknowledges the BYE request by sending a 200 OK to UE#1, which traverses back the signalling path.

11. Session host UE#1 shall tear down the message connection on the transport level and destroy local state for the message session. In case UE#1 does not use the IP-CAN bearer for any other service, it may decide to release the bearer.

12. UE#2 shall tear down the message connection on the transport level and destroy local state for the message session. In case UE#2 does not use the IP-CAN bearer for any other service, it may decide to release the bearer.

********** End of Change**********

3GPP TSG-SA WG2 Meeting #38
Atlanta , USA , February 16-20, 2004

Tdoc ⌘ S2-040968
revised from S2-040248, S2-040379

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **387** ⌘ **rev** **2** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	An optimisation in registration information flow for user not registered
Source:	⌘	SA2 (Huawei, China Mobile)
Work item code:	⌘	IMS2
Date:	⌘	19/02/2004
Category:	⌘	**F**
Release:	⌘	REL-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change: ⌘

In the registration information flow for user not registered, if only capabilities are returned in Cx-Query Resp, the I-CSCF will proceed to send Cx-Select-Pull (public user identity, private user identity) to the HSS to request the information related to the required S-CSCF capabilities, but the returned capabilities in Cx-Select-Pull Resp are the same with those returned in Cx-Query Resp, i.e., both shall satisfy the most restrictive service profile of the user which remains unchanged during this registration procedure. If I-CSCF cann't select an S-CSCF based on the capabilities returned in Cx-Query Resp, neither can the I-CSCF select an S-CSCF based on the capabilities returned in Cx-Select-Pull Resp. Therefore, the Cx-Select-Pull information flow is combined with the Cx-Query information flow.

In section 5.2.2.3, 5.2.2.4, and 5.12.1 of TS 23.228, when the S-CSCF sends Cx-Put to the HSS, the HSS only stores the S-CSCF name and returns Cx-Put Resp to acknowledge the sending of Cx-Put. Upon receipt of the Cx-Put Resp, the S-CSCF sends another information flow Cx-Pull to request to download the user profile information from the HSS. From the functional analysis view, the second interaction between the HSS and the S-CSCF is unnecessarily redundant. Furthermore, according to the description in section 6.1.2 of TS 29.228, the Cx-Put information flow and Cx-Pull information flow are the same Diameter command, which means the assignment/clearing of the S-CSCF name and the downloading of the user profile information to the S-CSCF can be finished in one information flow. Therefore, the current description in the TS 23.228 is incorrect and confusing.

In section 5.12.1 of TS 23.228, when the I-CSCF queries the HSS for current location information, the HSS responds with an indication that the Public User Indentity is unregistered for IMS in some cases. If the I-CSCF has not been

	provided with the location of the S-CSCF, it may send another information flow Cx-Select-Pull to the HSS to request the information related to the required S-CSCF capabilities which shall be input into the S-CSCF selection function. However according to the description in section 6.1.4 of TS 29.228, the required S-CSCF capabilities can be returned in the Cx-LocQuery Resp and the Cx-Select-Pull information flow is unnecessary. Therefore we suggest to delete the unnecessary information flow from the flow chart to achieve a clear and correct functionanlity description.
Summary of change: ⌘	During the registeration procedure for user not registered, Cx-Query Resp is sent from the HSS to the I-CSCF. When only capabilities are returned, the I-CSCF shall perform the new S-CSCF selection function based on the capabilities returned. The Cx-Query information flow and the Cx-Select-Pull information flow are combined. The Cx-Put information flow and the Cx-Pull information flow are combined in the Registration procedures and in the Mobile Terminating call procedures to unregistered Public User Identity that has services related to unregistered state. The Cx-Select-Pull information flow is deleted in the Mobile Terminating call procedures to unregistered Public User Identity that has services related to unregistered state.
Consequences if not approved: ⌘	The relationship between Cx-Query and Cx-Select-Pull, Cx-Put and Cx-Pull, Cx-LocQuery and Cx-Select-Pull are ambiguous and tend to cause confusion about the registration information flow.

Clauses affected:	⌘	5.2.2.3, 5.2.2.4, 5.12.1			
Other specs affected:	⌘	**Y**	**N**		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

How to create CRs using this form:

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

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

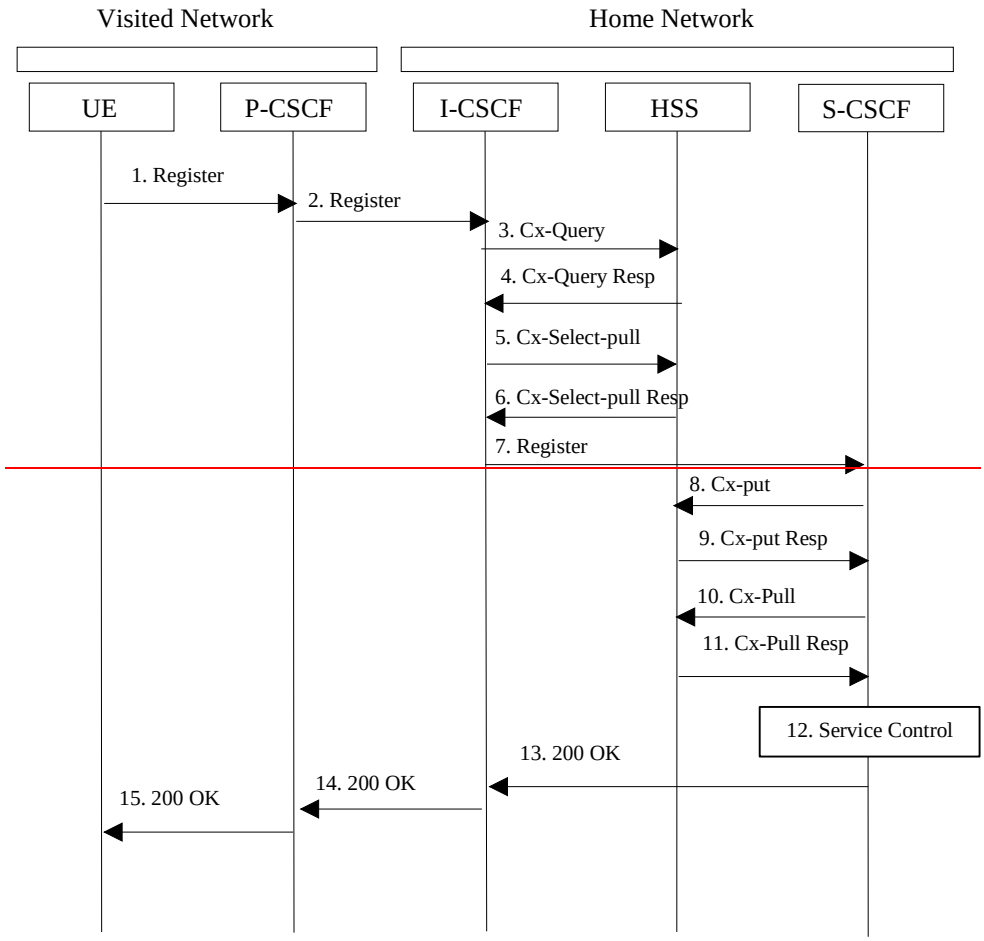
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest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

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

<< The first modification >>

5.2.2.3 Registration information flow – User not registered

The application level registration can be initiated after the registration to the access is performed, and after IP connectivity for the signalling has been gained from the access network. For the purpose of the registration information flows, the user is considered to be always roaming. For user roaming in their home network, the home network shall perform the role of the visited network elements and the home network elements.



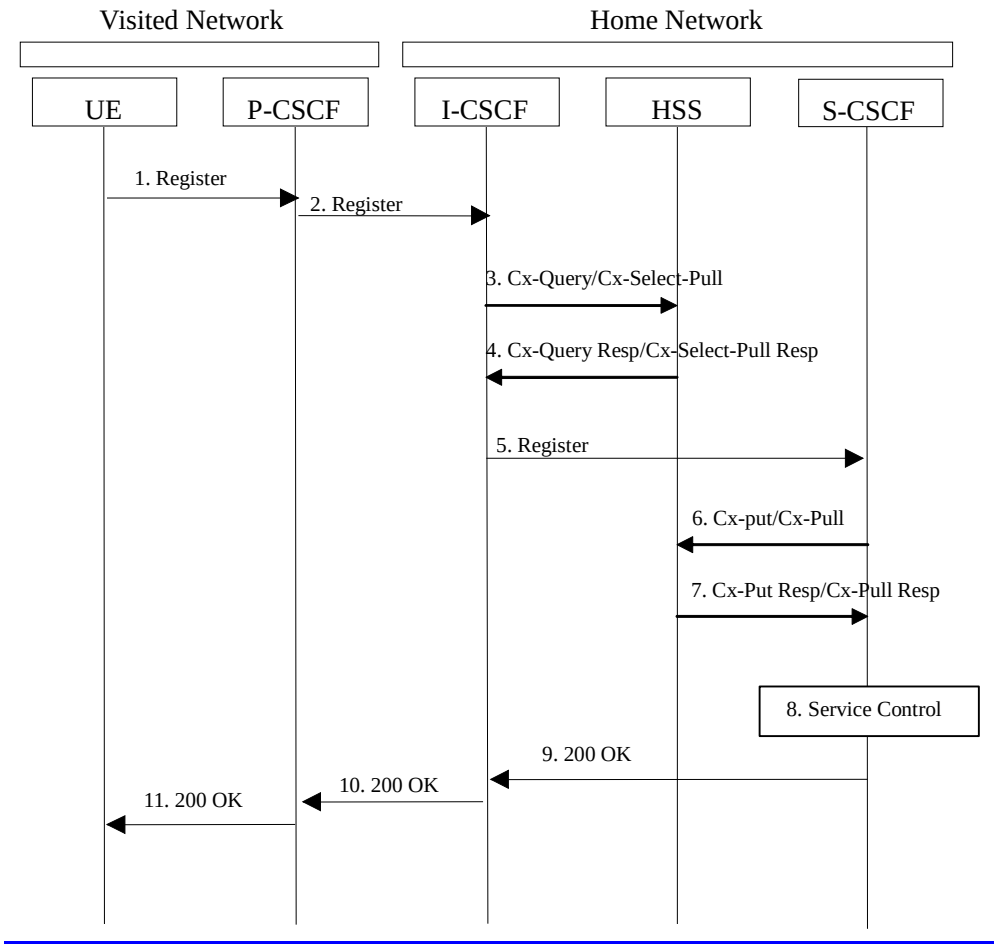


Figure 5.1: Registration – User not registered

1. After the UE has obtained IP connectivity, it can perform the IM registration. To do so, the UE sends the Register information flow to the proxy (public user identity, private user identity, home network domain name, UE IP address).

2. Upon receipt of the register information flow, the P-CSCF shall examine the “home domain name” to discover the entry point to the home network (i.e. the I-CSCF). The proxy shall send the Register information flow to the I-CSCF (P-CSCF address/name, public user identity, private user identity, P-CSCF network identifier, UE IP address). A name-address resolution mechanism is utilised in order to determine the address of the home network from the home domain name. The P-CSCF network identifier is a string that identifies at the home network, the network where the P-CSCF is located (e.g., the P-CSCF network identifier may be the domain name of the P-CSCF network).

3. The I-CSCF shall send the Cx-Query/Cx-Select-Pull information flow to the HSS (public user identity, private user identity, P-CSCF network identifier).

   The HSS shall check whether the user is registered already. The HSS shall indicate whether the user is allowed to register in that P-CSCF network (identified by the P-CSCF network identifier) according to the User subscription and operator limitations/restrictions if any.

4. Cx-Query Resp/Cx-Select-Pull Resp is sent from the HSS to the I-CSCF. It shall contain the S-CSCF name, if it is known by the HSS, and the S-CSCF capabilities, if it is necessary to select a new S-CSCF. When the response contains both S-CSCF name and capabilities the I-CSCF may perform a new assignment. When only capabilities are returned the I-CSCF shall perform the new S-CSCF selection function based on the capabilities returned.~~will continue proceeding according to step 5.~~

   If the checking in HSS was not successful the Cx-Query Resp shall reject the registration attempt.

~~5. If the I-CSCF has not been provided with the name of the S-CSCF then the I-CSCF shall send Cx-Select-Pull (public user identity, private user identity) to the HSS to request the information related to the required S-CSCF capabilities which shall be input into the S-CSCF selection function.~~

~~6. On receipt of the Cx-Select-Pull, the HSS shall send Cx-Select-Pull Resp (required S-CSCF capabilities) to the I-CSCF.~~

5~~7~~. The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism. The I-CSCF also determines the name of a suitable home network contact point, possibly based on information received from the HSS. The home network contact point may either be the S-CSCF itself, or a suitable I-CSCF(THIG) in case network configuration hiding is desired. If an I-CSCF(THIG) is chosen as the home network contact point for implementing network configuration hiding, it may be distinct from the I-CSCF that appears in this registration flow, and it shall be capable of deriving the S-CSCF name from the home contact information. I-CSCF shall then send the register information flow (P-CSCF address/name, public user identity, private user identity, P-CSCF network identifier, UE IP address, I-CSCF(THIG) in case network configuration hiding is desired) to the selected S-CSCF. The home network contact point will be used by the P-CSCF to forward session initiation signalling to the home network.

The S-CSCF shall store the P-CSCF address/name, as supplied by the visited network. This represents the address/name that the home network forwards the subsequent terminating session signalling to the UE. The S-CSCF shall store the P-CSCF Network ID information.

6~~8~~. The S-CSCF shall send Cx-Put/Cx-Pull (public user identity, private user identity, S-CSCF name) to the HSS. ~~The HSS stores the S-CSCF name for that user.~~

~~9. The HSS shall send Cx-Put Resp to the S-CSCF to acknowledge the sending of Cx-Put.~~

~~10. On receipt of the Cx-Put Resp information flow, the S-CSCF shall send the Cx-Pull information flow (public user identity, private user identity) to the HSS in order to be able to download the relevant information from the user profile to the S-CSCF. The S-CSCF shall store the P-CSCF address/name, as supplied by the visited network. This represents the address/name that the home network forwards the subsequent terminating session signalling to for the UE. The S-CSCF shall store the P-CSCF Network ID information.~~

7~~11~~. The HSS shall stores the S-CSCF name for that user and return the information flow Cx-Put Resp/Cx-Pull Resp (user information) to the S-CSCF. The user information passed from the HSS to the S-CSCF shall include one or more names/addresses information which can be used to access the platform(s) used for service control while the user is registered at this S-CSCF. The S-CSCF shall store the information for the indicated user. In addition to the names/addresses information, security information may also be sent for use within the S-CSCF.

8~~12~~. Based on the filter criteria, the S-CSCF shall send register information to the service control platform and perform whatever service control procedures are appropriate.

9~~13~~. The S-CSCF shall return the 200 OK information flow (home network contact information) to the I-CSCF. If an I-CSCF is chosen as the home network contact point for implementing network configuration hiding, the I-CSCF shall encrypt the S-CSCF address in the home network contact information.

10~~14~~. The I-CSCF shall send information flow 200 OK (home network contact information) to the P-CSCF. The I-CSCF shall release all registration information after sending information flow 200 OK.

11~~15~~. The P-CSCF shall store the home network contact information, and shall send information flow 200 OK to the UE.

Note: The encryption mechanism for implementing network configuration hiding is specified in TS 33.203.

5.2.2.4 Re-Registration information flow – User currently registered

Periodic application level re-registration is initiated by the UE either to refresh an existing registration or in response to a change in the registration status of the UE. Re-registration follows the same process as defined in subclause 5.2.2.3 “Registration Information Flow – User not registered”. When initiated by the UE, based on the registration time established during the previous registration, the UE shall keep a timer shorter than the registration related timer in the network.

Note: if the UE does not re-register, any active sessions may be deactivated.

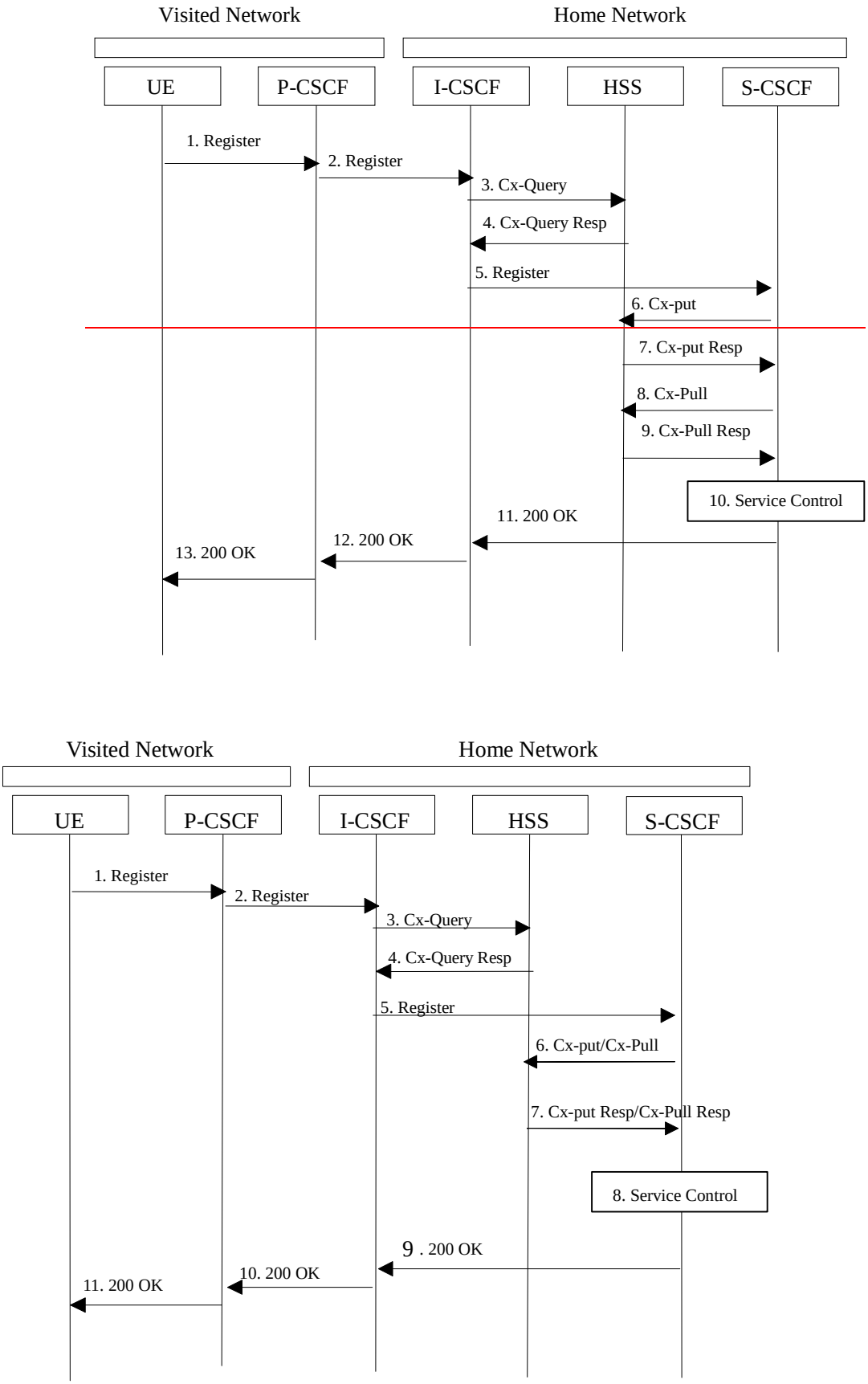


Figure 5.2: Re-registration - user currently registered

1. Prior to expiry of the agreed registration timer, the UE initiates a re-registration. To re-register, the UE sends a new REGISTER request. The UE sends the REGISTER information flow to the proxy (public user identity, private user identity, home network domain name, UE IP address).

2. Upon receipt of the register information flow, the P-CSCF shall examine the "home domain name" to discover the entry point to the home network (i.e. the I-CSCF). The proxy does not use the entry point cached from prior registrations. The proxy shall send the Register information flow to the I-CSCF (P-CSCF address/name, public user identity, private user identity, P-CSCF network identifier, UE IP address). A name-address resolution mechanism is utilised in order to determine the address of the home network from the home domain name. The P-CSCF network identifier is a string that identifies at the home network, the network where the P-CSCF is located (e.g., the P-CSCF network identifier may be the domain name of the P-CSCF network).

3. The I-CSCF shall send the Cx-Query information flow to the HSS (public user identity, private user identity and P-CSCF network identifier).

4. The HSS shall check whether the user is registered already and return an indication indicating that an S-CSCF is assigned. The Cx-Query Resp (indication of entry contact point, e.g. S-CSCF) is sent from the HSS to the I-CSCF.

5. The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism. The I-CSCF also determines the name of a suitable home network contact point, possibly based on information received from the HSS. The home network contact point may either be the S-CSCF itself, or a suitable I-CSCF(THIG) in case network configuration hiding is desired. If an I-CSCF(THIG) is chosen as the home network contact point for implementing network configuration hiding, it may be distinct from the I-CSCF that appears in this registration flow, and it shall be capable of deriving the S-CSCF name from the home contact information. I-CSCF shall then send the register information flow (P-CSCF address/name, public user identity, private user identity, P-CSCF network identifier, UE IP address, I-CSCF(THIG) in case network configuration hiding is desired) to the selected S-CSCF. The home network contact point will be used by the P-CSCF to forward session initiation signalling to the home network.

   The S-CSCF shall store the P-CSCF address/name, as supplied by the visited network. This represents the address/name that the home network forwards the subsequent terminating session signalling to the UE.

6. The S-CSCF shall send Cx-Put/Cx-Pull (public user identity, private user identity, S-CSCF name) to the HSS. ~~The HSS stores the S-CSCF name for that user.~~ Note: Optionally as an optimisation, the S-CSCF can detect that this is a re-registration and omit the Cx-Put/Cx-Pull request.

~~7. The HSS shall send Cx-Put Resp to the S-CSCF to acknowledge the sending of Cx-Put.~~

~~8. On receipt of the Cx-Put Resp information flow, the S-CSCF shall send the Cx-Pull information flow (public user identity, private user identity) to the HSS in order to be able to download the relevant information from the user profile to the S-CSCF. The S-CSCF shall store the P-CSCF address/name, as supplied by the visited network. This represents the address/name that the home network forwards the subsequent terminating session signalling to for the UE. Note: Optionally as an optimisation, the S-CSCF can detect that this a re-registration and omit the Cx-Pull request.~~

7~~9~~. The HSS shall stores the S-CSCF name for that user and return the information flow Cx-Put Resp/Cx-Pull-Resp (user information) to the S-CSCF. The S-CSCF shall store the user information for that indicated user.

8~~10~~. Based on the filter criteria, the S-CSCF shall send re-registration information to the service control platform and perform whatever service control procedures are appropriate.

9~~11~~. The S-CSCF shall return the 200 OK information flow (home network contact information) to the I-CSCF. If an I-CSCF is chosen as the home network contact point for implementing network configuration hiding, the I-CSCF shall encrypt the S-CSCF address in the home network contact information.

10~~12~~. The I-CSCF shall send information flow 200 OK (home network contact information) to the P-CSCF. The I-CSCF shall release all registration information after sending information flow 200 OK.

11~~13~~. The P-CSCF shall store the home network contact information, and shall send information flow 200 OK to the UE.

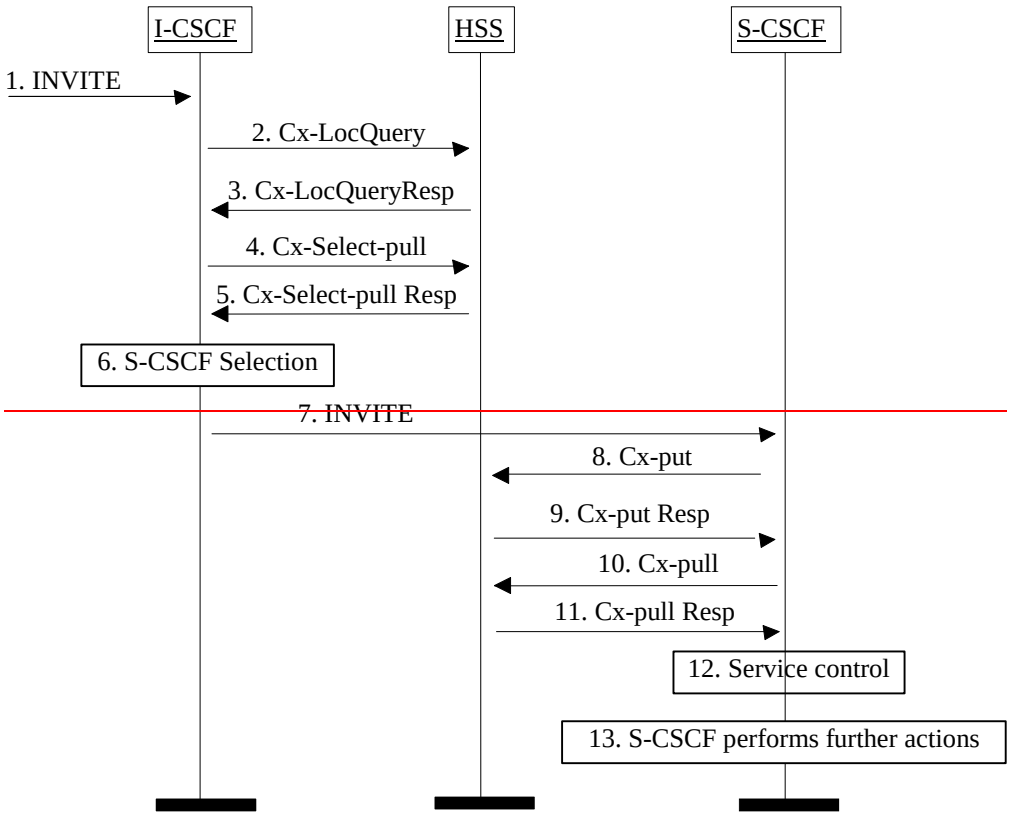
Note: The encryption mechanism for implementing network configuration hiding is specified in TS 33.203.

<< The second modification >>

5.12.1 Mobile Terminating call procedures to unregistered Public User Identity that has services related to unregistered state

In Figure 5.43 below the Public User Identity is unregistered for IMS and the Public User Identity has services related to unregistered state. In this case, the HSS responds back to I-CSCF with an indication that I-CSCF should select S-CSCF for this MT call to the unregistered Public User Identity of the user or provide the I-CSCF with the previously allocated S-CSCF name. Before S-CSCF selection, I-CSCF shall query HSS for the information related to the required S-CSCF capabilities. I-CSCF selects a S-CSCF to invoke service logic and I-CSCF routes the call further to the selected destination. If the S-CSCF does not have the relevant information from the user profile then the S-CSCF shall download the relevant information from HSS before it invokes service logic and any further actions in the call attempt. The service implemented by this information flow could be e.g. “Call Forward Unconditional.”

This is shown by the information flow in Figure 5.43:



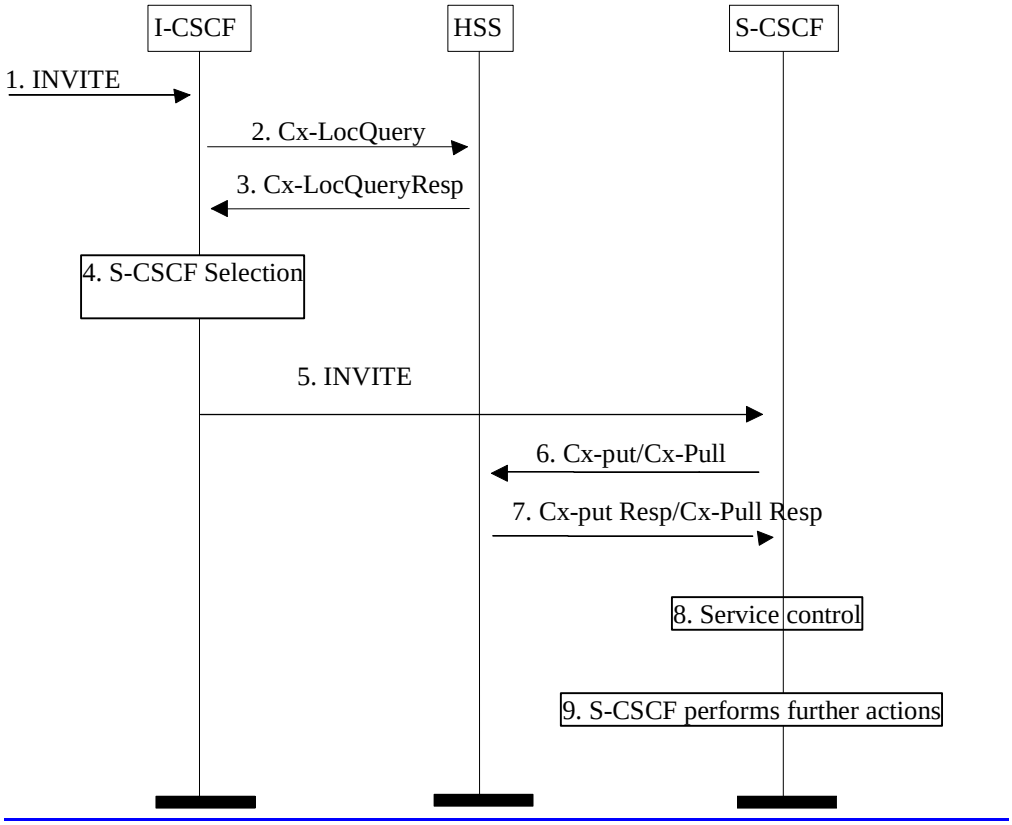


Figure 5.43: Mobile Terminating call procedures to unregistered IMS Public User Identity that has services related to unregistered state

1. I-CSCF receives an INVITE message.

2. I-CSCF queries the HSS for current location information.

3. HSS either responds with the required S-CSCF capabilities which ~~an indication that the Public User Identity is unregistered for IMS and~~ I-CSCF should use as an input to select a S-CSCF for the unregistered Public User Identity of the user or provides the I-CSCF with the previously allocated S-CSCF name for that user.

~~4. If the I-CSCF has not been provided with the location of the S-CSCF, the I-CSCF may send Cx-Select-Pull (unregistered, Public User Identity) to the HSS to request the information related to the required S-CSCF capabilities which shall be input into the S-CSCF selection function. This query is optional.~~

~~5. The HSS shall send Cx-Select-Pull Resp (required S-CSCF capabilities) to the I-CSCF.~~

4~~6~~. If the I-CSCF has not been provided with the location of the S-CSCF, the I-CSCF selects an S-CSCF for the unregistered Public User Identity of the user.

5~~7~~. I-CSCF forwards the INVITE request to the S-CSCF.

6~~8~~. The S-CSCF sends Cx-Put/Cx-Pull (Public User Identity, S-CSCF name) to the HSS. When multiple and separately addressable HSSs have been deployed by the network operator, then the S-CSCF needs to query the SLF to resolve the HSS. The HSS stores the S-CSCF name for unregistered Public User Identities of that user. This will result in all terminating traffic for unregistered Public User Identities of that user being routed to this particular S-CSCF until the registration period expires or the user attaches the Public User Identity to the network. Note: Optionally the S-CSCF can omit the Cx-Put/Cx-Pull request if it has the relevant information from the user profile.

~~9. The HSS shall send Cx-Put-Resp to the I-CSCF to acknowledge the sending of Cx-Put.~~

~~10. If the relevant information is not available, the S-CSCF shall send the Cx-Pull information flow (Public User Identity) towards the HSS in order to be able to download the relevant information of the service profile to the S-CSCF.~~

7~~11~~. The HSS shall stores the S-CSCF name for that user and return the information flow Cx-Put Resp/Cx-Pull Resp (user information) to the S-CSCF. The S-CSCF shall store it for that indicated Public User Identity.

8~~12~~. S-CSCF invokes whatever service logic is appropriate for this call attempt.

9~~13~~. S-CSCF performs whatever further actions are appropriate for this call attempt (in the case where the S-CSCF decides to redirect the session towards CS domain, the Mobile Termination Procedure MT#3 (section 5.7.2a) applies).

The S-CSCF may deregister the Public User Identity at any time (e.g. according to operator network engineering requirements) by issuing a Cx-Put2 (Public User Identity, clear S-CSCF name) clearing the S-CSCF name stored in the HSS. If S-CSCF name stored by the HSS does not match the name of the S-CSCF that originated the Cx-Put2 then the HSS will acknowledge the clearing request but take no further action.

3GPP TSG-SA WG2 Meeting #37 **Tdoc ⌘S2-040387**
Innsbruck, Austria, 12-16 January 2004

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **390** ⌘**rev** **1** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Registration and Public User Identity
Source:	⌘	SA2 (Siemens)
Work item code:	⌘	IMS2
Date:	⌘	13/01/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	The capability to register the same public user identity from multiple UEs has been added to Release 6. Though it has been described that these UEs would use different private user identities, the subclause on registration lacks guidance on the relationship to private user identities, not only, but especially for that case. There are also requirements in the subclause on implicit registration, which are not limited in scope to implicit registration.
Summary of change:	⌘	Add statement that registration and deregistration always relates to a particular private user identity.
Consequences if not approved:	⌘	Incomplete specification may cause misunderstandings.

Clauses affected:	⌘	5.2.1, 5.2.1a			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

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

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

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

5.2.1 Requirements considered for registration

The following points are considered as requirements for the purpose of the registration procedures.

1. The architecture shall allow for the Serving-CSCFs to have different capabilities or access to different capabilities. E.g. a VPN CSCF or CSCFs in different stages of network upgrade.

2. The network operator shall not be required to reveal the internal network structure to another network. Association of the node names of the same type of entity and their capabilities and the number of nodes will be kept within an operator's network. However disclosure of the internal architecture shall not be prevented on a per agreement basis.

3. A network shall not be required to expose the explicit IP addresses of the nodes within the network (excluding firewalls and border gateways).

4. It is desirable that the UE will use the same registration procedure(s) within its home and visited networks.

5. It is desirable that the procedures within the network(s) are transparent to the UE, when it register with the IM CN subsystem.

6. The Serving-CSCF is able to retrieve a service profile of the user who has IMS subscription.The Serving-CSCF knows how to reach the Proxy-CSCF currently serving the user who is registered.

7. The HSS shall support the possibility to bar a public user identity from being used for IMS non-registration procedures. The S-CSCF shall enforce these barring rules for IMS. Examples of use for the barring function are as follows:

   - Currently it is required that at least one public user identity shall be stored in the ISIM application. In case the user/operator wants to prevent this public user identity from being used for IMS communications, it shall be possible to do so in the network without affecting the ISIM application directly.

8. The HSS shall support the possibility to restrict a user from getting access to IM CN Subsystem from unauthorized visited networks.

9. It shall be possible to register multiple public identities via single IMS registration procedure from the UE. See subclause 5.2.1a for details.

10. It shall be possible to register a Public User Identity that is simultaneously shared across multiple contact addresses via IMS registration procedures. However, each registration and each de-registration process always relates to a particular contact address and a particular private user identity.

11. Registration of a public user identity shall not affect the status of already registered public user identity(s), unless due to requirements by Implicit Registration set defined in subclause 5.2.1a.

12. When multiple UEs share the same public identity (es), each UE shall be able to register its contact address with IMS.

13. The UE may indicate its capabilities and characteristics in terms of SIP User Agent capabilities and characteristics described in "draft-ietf-sip-callee-caps-01" [38] during IMS registration.

5.2.1a Implicit Registration

When an user has a set of public user identities defined to be implicitly registered via single IMS registration of one of the public user identity's in that set, it is considered to be an Implicit Registration. No single public identity shall be considered as a master to the other public user identities. Figure 5.2.1a shows a simple diagram of implicit registration and public user identities. In order to support this function, it is required that:

- HSS has the set of public user identities that are part of implicit registration.
- Cx reference point between S-CSCF and HSS shall support download of all public user identities associated with the implicit registration, during registration of any of the single public user identities within the set.

- All public user identities of an Implicit Registration set must be associated to the same private user identities. See figure 5.2.1.b for the detailed relationship between the public and private user entities within an Implicit Registration set.
- When one of the public user identities within the set is registered, all Public user identities associated with the implicit registration set are registered at the same time.
- When one of the public user identities within the set is de-registered, all public user identities that have been implicitly registered are de-registered at the same time.
- Registration and de-registration always relates to a particular contact address and a particular private user identity. A Public user identi~~i~~ty that has been registered (including when implicitly registered) with different contact addresses remains registered in relation to those contact addresses that have not been de-registered.
- Public user identities belonging to an implicit registration set may point to different service profiles; or some of these public user identities may point to the same service profile.
- When a public user identity belongs to an implicit registration set, it cannot be registered or de-registered individually without the public user identity being removed from the implicit registration list.
- All IMS related registration timers should apply to the set of implicitly registered public user identities
- S-CSCF, P-CSCF and UE shall be notified of the set of public user identities belonging to the implicitly registered function. Session set up shall not be allowed for the implicitly registered public user identities until the entities are updated, except for the explicitly registered public user identity.
- The S-CSCF shall store during registration all the Service profiles corresponding to the public user identities being registered.
- When a public user identity is barred from IMS communications, only the HSS and S-CSCF shall have access to this public user identity.

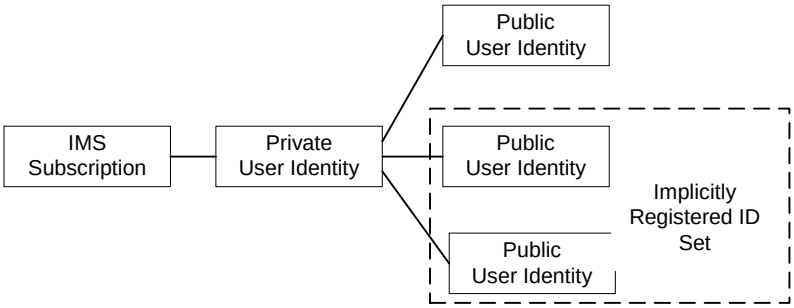


Figure 5.2.1a Relationship of public user identities when implicitly registered

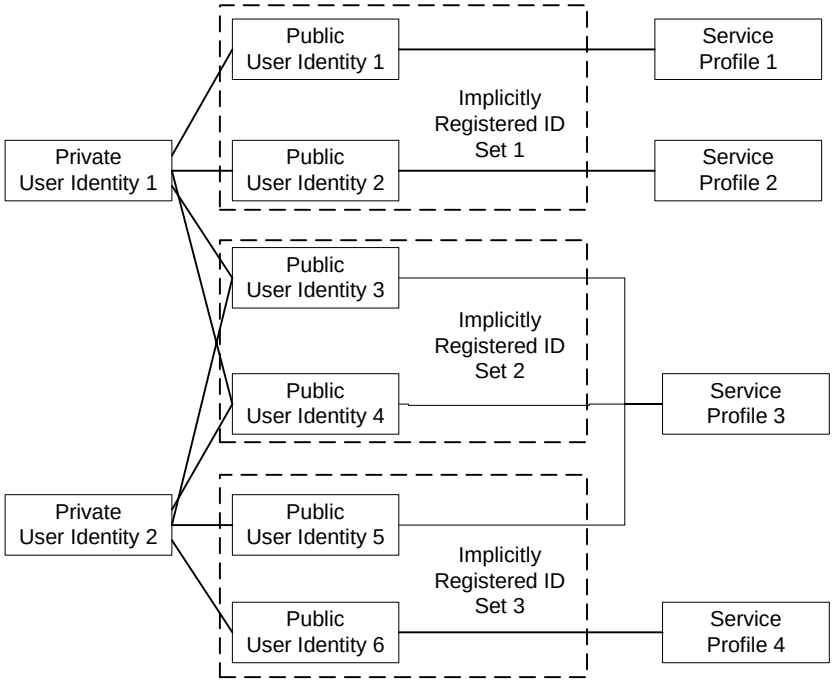


Figure 5.2.1.b – The relation of two shared Public User Identities (Public-ID-3 and 4) and Private User Identities

5.2.1a.1 Implicit Registration for UE without ISIM

In case an UE is registering in the IMS without ISIM, it shall require the network's assistance to register atleast one public user identity, which is used for session establishment & IMS signalling. Implicit registration shall be used as part of a mandatory function for these ISIM-less UEs to register the public user identity(s). In addition to the functions defined in section 5.2.1a, the following additional functions are required for this scenario.

- The Temporary public identity shall be used for initial registration process
- It shall be defined in HSS that if the user does not have implicit registration activated then the user shall not be allowed to register in the IMS using the Temporary public user identity.

3GPP TSG-SA WG2 Meeting #38
Atlanta, USA, 16-20 February 2004

Tdoc ⌘S2-040954

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **391** ⌘**rev** **5** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Record Route at S-CSCF
Source:	⌘	SA2 (Siemens)
Work item code:	⌘	IMS2
Date:	⌘	17/02/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	Currently all SIP signalling for a UE traverses the S-CSCF assigned to the UE at registration time. More specifically, record-route in the S-CSCF guarantees that all following requests within a dialogue go through the S-CSCF. On one hand this guarantees a central point of control in the home network, on the other hand it may create considerable load in the S-CSCF (e.g. if all presence notifications go through the S-CSCF of a presentity). Thus though the current specification is desirable for multimedia telephony-type services, it may not be applicable for all services, in particular if there is an AS in the operator domain in control of the session. One important example is the Presence service.
Summary of change:	⌘	Allow the option to configure the S-CSCF not to record-route. Enhance subclause 5.4.5 to provide the necessary context. Add a new informative annex to give some background information to assist the reader.
Consequences if not approved:	⌘	Unnecessary load to S-CSCF.

Clauses affected:	⌘	5.4.5, new informative annex F

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

Other comments: ⌘

How to create CRs using this form:

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

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

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

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

*** FIRST CHANGE ***

5.4.5 ~~Storing of s~~Session P~~p~~ath I~~i~~nformation

5.4.5.1 Session Path Information during Registration and Session Initiation

During registration and session initiation there are SIP mechanisms, which provide the means to determine the session path.

After registration the P-CSCF stores the S-CSCF name and the S-CSCF stores the P-CSCF name (see 4.3.4) as part of the UE related information.

There is a need to store the session path that is determined during the session initiation request in order to route the subsequent session requests through this determined path. This is needed in order to route these session requests through certain nodes, e.g. the ones performing Service Control. CSCFs are assumed to perform certain actions:

1. CSCFs (Proxy and Serving) store a certain part of the session path determined during session initiation. This allows CSCFs to generate requests that traverse all elements on a Route path.

2. ~~–~~The P-CSCF shall check correct usage of the header values. Should an UE build inaccurate header(s) in a SIP request, the P-CSCF may reject the request. If an operator policy requires enforcing the routes stored in P-CSCF, the P-CSCF shall overwrite the header(s) provided by the UE with the appropriate values.

5.4.5.2 P-CSCF in the Session Path

All SIP signalling to or from the UE traverses the P-CSCF.

5.4.5.3 S-CSCF in the Session Path

All initial requests to or from the UE traverse the S-CSCF assigned to the UE. The S-CSCF uses the "Record-Route" mechanism defined in RFC 3261 [12] to remain in the signalling path for subsequent requests too; in short terms: the S-CSCF "record-routes". This is considered the default behaviour for all IMS communication. However, if Application Servers under operator control guarantee the home control of the session, then it may not be required that all subsequent requests traverse the S-CSCF. In such cases the operator may choose that the S-CSCF does not "record-route". The detailed record-route behaviour is configured in the S-CSCF, e.g. on a per-service basis. The S-CSCF decides whether it performs record-routing or not based on operator configuration in the S-CSCF.

See also Annex F for background information.

*** NEXT CHANGE ***

Annex F (informative): Routing subsequent requests through the S-CSCF

This annex provides some background information related to subclause 5.4.5.3.

The S-CSCF is the focal point of home control. It guarantees operator control over sessions. Therefore IMS has been designed to guarantee that all initial session signalling requests goes through the Home S-CSCF on both terminating and originating side. A number of tasks performed by the S-CSCF are performed either at registration time or immediately during session set-up, e.g. evaluation of initial filter criteria. However, there are tasks of the S-CSCF, which require the presence of the S-CSCF in the signalling path afterwards:

- Media parameter control: If the S-CSCF finds media parameters that local policy or the user's subscriber profile does not allow to be used within an IMS session, it informs the originator. This requires record-routing in the S-CSCF. For example, change of media parameters using UPDATE would by-pass a S-CSCF, which does not record-route.

- CDR generation: The S-CSCF generates CDRs, which are used for offline charging and for statistical purposes. A S-CSCF, which does not record-route, would not even be aware of session termination. If the CDRs at the S-CSCF are needed, then the S-CSCF must record-route.

- Network initiated session release: The S-CSCF may generate a network-initiated session release, e.g. for administrative reasons. For that purpose a S-CSCF needs to be aware of ongoing sessions. In particular it must be aware of hard state dialogs that are required to be terminated by an explicit SIP request.

The above criteria are particularly important for "multimedia telephony" type peer-to-peer communication.

- Media parameter control guarantees that the user does not use services he or she did not pay for.

- For telephony type services the session charging component is the most important one.

- If a subscriber is administratively blocked, the network shall have the possibility to terminate ongoing communication.

More generally, all the tasks are needed; thus they need to be provided elsewhere if the S-CSCF does not record-route.

On the other hand there are client-server based services, which may be offered by the home operator. An example of such service available today where the no record route principle is applied, is Presence, where notifications need not go through the S-CSCF. Another example could be where the UE initiates a session to an Application Server (AS) in the home operator's domain, e.g. video download. In such cases:

- The server implementation (or the server’s knowledge of user subscription data) may limit the allowed media parameters.

- Charging will be mostly event-based charging (content charging) and depends on the information provided from the AS.

- The AS can terminate sessions. And the dialogs may be soft state dialogs, which are not required to be terminated by an explicit SIP request (e.g. SUBSCRIBE dialogs).
  However not in all cases the AS would receive the necessary information, which usually triggers session release (e.g. for administrative reasons).

Thus, for some client-server based services, it might not be necessary to keep the S-CSCF in the path. It may be desirable for an operator to avoid the load in the S-CSCF and control the service from the AS. For such services "no record-routing in S-CSCF" may be configured together with the initial filter criteria, as defined in subclause 5.4.5.3.

Annex ~~F~~ G (informative): Change history

3GPP TSG-SA WG-2 Meeting #37
Innsbruck, Austria, 12-16 January 2004

Tdoc ⌘S2-040398

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **393** ⌘**rev** **1** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Alignment of headings with drafting rules
Source:	⌘	SA2 (Lucent)
Work item code:	⌘	IMS2
Date:	⌘	12/01/2004
Category:	⌘	**D**
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The specification does not follow the drafting rules with respect to use of clauses and sub-clauses. Also an incorrect acronym was found.
Summary of change:	⌘	Add headings to prevent clauses with sub-clauses from also containing text and change incorrect acronym.
Consequences if not approved:	⌘	Non-conformance with drafting rules.

Clauses affected:	⌘	3.3, 4.0, 4.2.5.1, 4.3.3.0, 4.6.0, 4.6.2.0, 4.10.0, 5.0, 5.1.1.0, 5.1.5.0, 5.2.0, 5.2.1a.0, 5.3.2.0, 5.3.2.2.0, 5.4.0, 5.4.6.0, 5.4.7.0, 5.4.9.0, 5.4.12.0, 5.5.0, 5.6.0, 5.7.0, 5.8.0, 5.10.0, 5.10.3.1.0, 5.11.1.0, 5.11.2.0, 5.11.3.0, 5.11.4.0, 5.11.5.0, 5.11.6.0, 5.11.6.2.0, 5.12.0, 5.13.0, 5.14.0, 5.15.0, 5.16.0, 5.16.1.0, 5.16.1.1.0, 5.16.2.0, 5.16.2.2.0, 5.18.0, E.0, E.1.0, E.1.1.0, E.2.1.0, E.2.2.0, E.2.3.0, and E.2.4.0

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

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

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

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

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

**** First Change ****

3.3 Abbreviations

For the purposes of the present document the following abbreviations apply. Additional applicable abbreviations can be found in GSM 01.04 [1].

AMR	Adaptive Multi-rate
API	Application Program Interface
AS	Application Server
BCSM	Basic Call State Model
BG	Border Gateway
BGCF	Breakout Gateway Control Function
BS	Bearer Service
CAMEL	Customised Application Mobile Enhanced Logic
CAP	Camel Application Part
CDR	Charging DataRecord
CN	Core Network
CS	Circuit Switched
CSCF	Call Session Control Function
CSE	CAMEL Service Environment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ENUM	E.164 Number
GGSN	Gateway GPRS Support Node
GMLC	Gateway Mobile Location Centre
GUP	Generic User Profile
HSS	Home Subscriber Server
I-CSCF	Interrogating-CSCF
IETF	Internet Engineering Task Force
IM	IP Multimedia
~~IM CN SS~~	~~IP Multimedia Core Network Subsystem~~
IMS	IP Multimedia Core Network Subsystem
IMS ALG	IMS Application Level Gateway
IMSI	International Mobile Subscriber Identifier
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IP-CAN	IP-Connectivity Access Network
ISDN	Integrated Services Digital Network
ISIM	IMS SIM
ISP	Internet Service Provider
ISUP	ISDN User Part
MAP	Mobile Application Part
MGCF	Media Gateway Control Function
MGF	Media Gateway Function
NAI	Network Access Identifier
NA(P)T-PT	Network Address (Port-Multiplexing) Translation-Protocol Translation
OSA	Open Services Architecture
P-CSCF	Proxy-CSCF
PDF	Policy Decision Function
PDN	Packet Data Network
PDP	Packet Data Protocol e.g., IP
PEF	Policy Enforcement Function
PLMN	Public Land Mobile Network
PSI	Public Service Identity
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAB	Radio Access Bearer
RFC	Request for Comments

**** Next Change ****

4 IP multimedia subsystem concepts

4.0 General

The IP Multimedia CN subsystem comprises all CN elements for provision of multimedia services. This includes the collection of signalling and bearer related network elements as defined in TS 23.002 [1]. IP multimedia services are based on an IETF defined session control capability which, along with multimedia bearers, utilises the IP-Connectivity Access Network (this may include an equivalent set of services to the relevant subset of CS Services).

In order to achieve access independence and to maintain a smooth interoperation with wireline terminals across the Internet, the IP multimedia subsystem attempts to be conformant to IETF “Internet standards”. Therefore, the interfaces specified conform as far as possible to IETF “Internet standards” for the cases where an IETF protocol has been selected, e.g. SIP.

The IP multimedia core network (IM CN) subsystem enables PLMN operators to offer their subscribers multimedia services based on and built upon Internet applications, services and protocols. There is no intention here to standardise such services within the IM CN subsystem, the intention is that such services will be developed by PLMN operators and other third party suppliers including those in the Internet space using the mechanisms provided by the Internet and the IM CN subsystem. The IM CN subsystem should enable the convergence of, and access to, voice, video, messaging, data and web-based technologies for the wireless user, and combine the growth of the Internet with the growth in mobile communications.

The complete solution for the support of IP multimedia applications consists of terminals, IP-Connectivity Access Networks (IP-CAN), and the specific functional elements of the IM CN subsystem described in this technical specification. An example of IP-Connectivity Access Network is the GPRS core network with GERAN and/or UTRAN radio access networks.

4.1 Relationship to CS domain and the IP-Connectivity Access Network

The IP multimedia subsystem utilizes the IP-CAN to transport multimedia signalling and bearer traffic. The IP-CAN maintains the service while the terminal moves and hides these moves from the IP multimedia subsystem.

The IP multimedia subsystem is independent of the CS domain although some network elements may be common with the CS domain. This means that it is not necessary to deploy a CS domain in order to support an IP multimedia subsystem based network.

**** Next Change ****

4.2.5 The QoS requirements for an IM CN subsystem session

The selection, deployment, initiation and termination of QoS signalling and resource allocation shall consider the following requirements so as to guarantee the QoS requirement associated with an IM CN subsystem session.

1. Independence between QoS signalling and Session Control

The selection of QoS signalling and resource allocation schemes should be independent of the selected session control protocols. This allows for independent evolution of QoS control and the session control in the IM CN subsystem.

2. Necessity for End-to-End QoS Signalling and Resource -Allocation

   End-to-end QoS indication, negotiation and resource allocation during the session set-up in the IM CN subsystem should be enforced for those services and applications that require QoS better than best-effort.

4. Restricted Resource Access at the IP BS Level

   Access to the resources and provisioning of QoS at IP BS Level should be authenticated and authorised by applying appropriate QoS policies via the IP Policy Control element

5. Restricted Resource Access at the IP-Connectivity Access Network (i.e. layer-2) Level

   Access to the resources and provisioning of QoS at the IP-Connectivity Access Network Level should be authenticated and authorised by using existing registration/security/QoS policy control mechanisms of the IP-CAN.

6. Co-ordination between Session Control and QoS Signalling/Resource Allocation

   a. In establishing an IMS session, it shall be possible for an application to request that the resources needed for bearer establishment be successfully allocated before the destination user is alerted.

   b. In establishing an IMS session, it shall be possible, dependent on the application being offered, to prevent the use of the bearer until the session establishment is completed.

   c. In establishing an IMS session, it shall be possible for a terminating application to allow the destination user to participate in determining which bearers shall be established.

   d. Successful bearer establishment shall include the completion of any required end-to-end QoS signalling, negotiation and resource allocation

   The initiation of any required end-to-end QoS signalling, negotiation and resource allocation processes at different network segments shall take place after the initiation and delivery of a session set-up request.

7. The Efficiency of QoS Signalling and Resource Allocation

   The sequence of end-to-end QoS signalling, negotiation and resource allocation processes at different network segments should primarily consider the delay in negotiating end-to-end QoS and reserving resources that contributes to the session set-up delay. Parallel or overlapping QoS negotiation and resource reservation shall be allowed where possible.

8. Dynamic QoS Negotiation and Resource Allocation

   Changes (upgrading or downgrading) of QoS provided to an active IMS session shall be supported based on either the request from the IM application or the current network loads or link quality (e.g. radio link quality).

   It shall be possible to maintain a resource allocation in excess of the resources needed for current media flows (but within the restrictions imposed by points #4 and #5 above), in order to e.g. switch to different media flow characteristics without risk of admission control failure.

9 Prevention of Theft of Service

   The possibility for theft of service in the IM CN subsystem shall be no higher than that for the corresponding packet data and circuit switched services.

10 Prevention of Denial of Service

   The system unavailability due to denial of service attacks in the IM CN subsystem shall be no greater than that for the corresponding packet data and circuit switched services.

~~4.2.5.1 Void~~

4.2.6 QoS Requirements for IM CN subsystem signalling

The UE shall be able to establish a dedicated signalling IP-CAN bearer for IM Subsystem related signalling or utilize a general-purpose IP-CAN bearer for IM subsystem signalling traffic.

The use of a dedicated signalling IP-CAN bearer for IM Subsystem related signalling may provide enhanced QoS for signalling traffic.

If a dedicated signalling IP-CAN bearer is to be used for IM Subsystem related signalling, rules and restrictions may apply to the bearer according to operator implementation. A set of capabilities shall be standardised to provide user experience consistency and satisfy user expectation. The rules and restrictions on other capabilities beyond the standardised set are configured by the operator in the IP-CAN.

To enable the described mechanism to work without requiring end-user interaction and under roaming circumstances, it is a requirement for the UE to be made aware of the rules and restrictions applied by the visited network operator. As there is as yet no mechanism available in this Release for providing the information about the restrictions back to the UE, the available set of rules and restrictions in this Release is the set of capabilities as defined below.

The dedicated signalling IP-CAN bearer is subject to restrictions, the capabilities to be applied are defined as follows: all messages from the UE that use a dedicated signalling IP-CAN bearer shall have their destination restricted to:

-the P-CSCF assigned for this UE, or to any one of the set of possible P-CSCFs that may be assigned to this UE

-and towards DHCP and DNS servers within the IMS operator's domain where the P-CSCF is located.

The UE is not trusted to implement these restrictions, therefore the restrictions are enforced in the IP-CAN by the operator.

The IP-CAN shall be able to apply rules and restrictions for the IM CN subsystem traffic. In particular, the IP-CAN shall be able to identify IM CN subsystem signalling traffic in order for the operator to decide on what particular rating to apply to the IM CN subsystem signalling traffic. This includes the ability to apply a special rating to at least SIP, DHCP, DNS and HTTP traffic for IMS.

**** Next Change ****

4.3.3 Identification of users

4.3.3.0 General

There are various identities that may be associated with a user of IP multimedia services. This section describes these identities and their use.

4.3.3.1 Private user identities

Every IM CN subsystem user shall have one or more private user identities. The private identity is assigned by the home network operator, and used, for example, for Registration, Authorisation, Administration, and Accounting purposes. This identity shall take the form of a Network Access Identifier (NAI) as defined in RFC 2486 [14]. It is possible for a representation of the IMSI to be contained within the NAI for the private identity.

- The Private User Identity is not used for routing of SIP messages.
- The Private User Identity shall be contained in all Registration requests, (including Re-registration and De-registration requests) passed from the UE to the home network.
- An ISIM application shall securely store one Private User Identity. It shall not be possible for the UE to modify the Private User Identity information stored on the ISIM application.

- The Private User Identity is a unique global identity defined by the Home Network Operator, which may be used within the home network to uniquely identify the user from a network perspective.
- The Private User Identity shall be permanently allocated to a user (it is not a dynamic identity), and is valid for the duration of the user's subscription with the home network.
- The Private User Identity is used to identify the user's information (for example authentication information) stored within the HSS (for use for example during Registration).
- The Private User Identity may be present in charging records based on operator policies.
- The Private User Identity identifies the subscription (e.g. IM service capability) not the user.
- The Private User Identity is authenticated only during registration of the user, (including re-registration and de-registration).
- The HSS needs to store the Private User Identity.
- The S-CSCF needs to obtain and store the Private User Identity upon registration and unregistered termination.

**** Next Change ****

4.6 Roles of Session Control Functions

4.6.0 General

The CSCF may take on various roles as used in the IP multimedia subsystem. The following sections describe these various roles.

4.6.1 Proxy-CSCF

The Proxy-CSCF (P-CSCF) is the first contact point within the IM CN subsystem. Its address is discovered by UEs using the mechanism described in section "Procedures related to Local CSCF Discovery ". The P-CSCF behaves like a Proxy (as defined in RFC 3261 [12] or subsequent versions), i.e. it accepts requests and services them internally or forwards them on. The P-CSCF shall not modify the Request URI in the SIP INVITE message. The P-CSCF may behave as a User Agent (as defined in the RFC 3261 [12] or subsequent versions), i.e. in abnormal conditions it may terminate and independently generate SIP transactions.

The Policy Decision Function (PDF) is a logical entity of the P-CSCF. If the PDF is implemented in a separate physical node, the interface between the PDF and the P-CSCF is not standardised.

The functions performed by the P-CSCF are:

- Forward the SIP register request received from the UE to an I-CSCF determined using the home domain name, as provided by the UE.
- Forward SIP messages received from the UE to the SIP server (e.g. S-CSCF) whose name the P-CSCF has received as a result of the registration procedure.
- Forward the SIP request or response to the UE.

Detect and handle an emergency session establishment request as per error handling procedures defined by stage-3.

- Generation of CDRs.
- Maintain a Security Association between itself and each UE, as defined in TS 33.203 [19].
- Should perform SIP message compression/decompression.

- Authorisation of bearer resources and QoS management. For details see TS 23.207 [9].

4.6.2 Interrogating-CSCF

4.6.2.0 General

Interrogating-CSCF (I-CSCF) is the contact point within an operator's network for all connections destined to a user of that network operator, or a roaming user currently located within that network operator's service area. There may be multiple I-CSCFs within an operator's network. The functions performed by the I-CSCF are:

Registration

- Assigning a S-CSCF to a user performing SIP registration (see section on Procedures related to Serving-CSCF assignment)

Session-related and session-unrelated flows

- Route a SIP request received from another network towards the S-CSCF.
- Obtain from HSS the Address of the S-CSCF.
- Forward the SIP request or response to the S-CSCF determined by the step above

Charging and resource utilisation:

- Generation of CDRs.

4.6.2.1 Topology Hiding Inter-network Gateway

In performing the above functions the operator may use a Topology Hiding Inter-network Gateway (THIG) function in the I-CSCF (referred to hereafter as I-CSCF(THIG)) or other techniques to hide the configuration, capacity, and topology of the network from the outside. When an I-CSCF(THIG) is chosen to meet the hiding requirement then for sessions traversing across different operators domains, the I-CSCF(THIG) may forward the SIP request or response to another I-CSCF(THIG) allowing the operators to maintain configuration independence.

**** Next Change ****

4.10 IMS group management concepts

4.10.0 General

This clause describes architectural concepts to fulfil the requirements for IMS Group Management described in TS 22.250 [32].

4.10.1 IMS group administration

The capabilities required for IMS group management are defined in clause 5.4 of TS 22.250 [32]. The Ut reference point is used to manage groups from the UE. This does not preclude the use of other mechanisms for group management, e.g. using OSA or OA&M mechanisms; the details of these other mechanisms are out of scope of this document.

4.10.2 Group identifiers

Each group shall be addressable by a globally unique group identifier. The group identifier shall take the form of a Public Service Identifier.

4.11 Relationship to 3GPP Generic User Profile (GUP)

It shall be possible to apply the mechanisms and format of the 3GPP Generic User Profile (GUP) to IM CN Subsystem user related data. The 3GPP Generic User Profile (GUP) is described in 3GPP TS 23.240 [31].

5 IP multimedia subsystem procedures

5.0 General

This section documents the main procedures that are used for the provision of services in the IP multimedia subsystem. These procedures are described using text description as well as information flow diagrams. The procedures described in this document are meant to provide a high level description and are not intended to be exhaustive. Additional procedures and details are provided in TS 24.228 [10].

In the following sections, user roaming procedures apply to cases where P-CSCF is located in the visited network. Procedures for cases where the user is roaming and the P-CSCF is located in the home network are similar to procedures for a non-roaming user.

5.0a Session-unrelated procedures

The IM CN Subsystem provides means to conduct session-unrelated interactions between users, e.g. OPTIONS query, outband REFER. These interactions are described in RFC 3261 [12], and other possible RFCs.

These interactions shall use and fully comply with the basic mechanisms described for session-related procedures of the IM CN Subsystem. These mechanisms include e.g.routing, security, service control, network hiding as described in other sections and specifications.

5.1 CSCF related procedures

5.1.0 Establishing IP-Connectivity Access Network bearer for IM CN Subsystem Related Signalling

Before the UE can request IM services, an appropriate IP-CAN bearer must be available to carry IM Subsystem related signalling.

5.1.1 Procedures related to local CSCF discovery

5.1.1.0 General

The Proxy-CSCF discovery shall be performed using one of the following mechanisms:

- As part of the establishment of connectivity towards the IP-Connectivity Access Network, if the IP-Connectivity Access Network provides such means.

- Alternatively, the P-CSCF discovery may be perfomed after the IP connectivity has been established. To enable P-CSCF discovery after the establishment of IP connectivity, the IP-Connectivity Access Network shall provide the following P-CSCF discovery option to the UE:

Use of DHCP to provide the UE with the domain name of a Proxy-CSCF and the address of a Domain Name Server (DNS) that is capable of resolving the Proxy-CSCF name, as described below in clause 5.1.1.1.

5.1.1.1 DHCP/DNS procedure for P-CSCF discovery

The DHCP relay agent within the IP-Connectivity Access Network relays DHCP messages between UE and the DHCP server.

**** Next Change ****

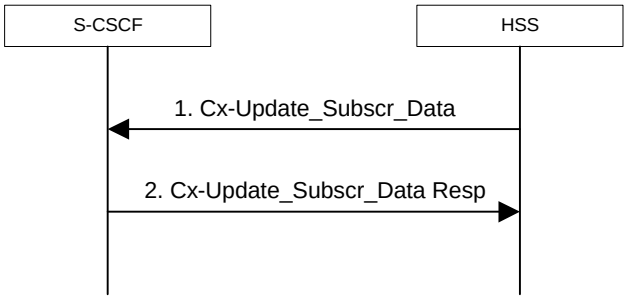
5.1.5 Subscription Updating Procedures

5.1.5.0 General

Whenever a modification has occurred in the subscription data that constitutes the data used by the S-CSCF, the complete subscription data set shall be sent to the S-CSCF by the HSS. HSS shall use the Push model for downloading the subscription data to the S-CSCF.

5.1.5.1 Subscription updating information flow

This section provides the information flows for subscription data updating procedure.



1. The HSS sends the Cx-Update_Subscr_Data with the subscription data to the S-CSCF.
2. The S-CSCF sends Cx-Update_Subscr_Data Resp to the HSS to acknowledge the sending of Cx-Update_Subscr_Data

5.2 Application level registration procedures

5.2.0 General

The following sub-sections address requirements and information flows related to registration in the IP multimedia subsystem. Assumptions that apply to the various information flows are listed as appropriate.

5.2.1 Requirements considered for registration

The following points are considered as requirements for the purpose of the registration procedures.

1. The architecture shall allow for the Serving-CSCFs to have different capabilities or access to different capabilities. E.g. a VPN CSCF or CSCFs in different stages of network upgrade.
2. The network operator shall not be required to reveal the internal network structure to another network. Association of the node names of the same type of entity and their capabilities and the number of nodes will be kept within an operator's network. However disclosure of the internal architecture shall not be prevented on a per agreement basis.
3. A network shall not be required to expose the explicit IP addresses of the nodes within the network (excluding firewalls and border gateways).
4. It is desirable that the UE will use the same registration procedure(s) within its home and visited networks.
5. It is desirable that the procedures within the network(s) are transparent to the UE, when it register with the IM CN subsystem.

6. The Serving-CSCF is able to retrieve a service profile of the user who has IMS subscription.The Serving-CSCF knows how to reach the Proxy-CSCF currently serving the user who is registered.

7. The HSS shall support the possibility to bar a public user identity from being used for IMS non-registration procedures. The S-CSCF shall enforce these barring rules for IMS. Examples of use for the barring function are as follows:

   - Currently it is required that at least one public user identity shall be stored in the ISIM application. In case the user/operator wants to prevent this public user identity from being used for IMS communications, it shall be possible to do so in the network without affecting the ISIM application directly.

8. The HSS shall support the possibility to restrict a user from getting access to IM CN Subsystem from unauthorized visited networks.

9. It shall be possible to register multiple public identities via single IMS registration procedure from the UE.

10. It shall be possible to register a Public User Identity that is simultaneously shared across multiple contact addresses via IMS registration procedures.

11. Registration of a public user identity shall not affect the status of already registered public user identity(s), unless due to requirements by Implicit Registration set defined in subclause 5.2.1a.

12. When multiple UEs share the same public identity (es), each UE shall be able to register its contact address with IMS.

13. The UE may indicate its capabilities and characteristics in terms of SIP User Agent capabilities and characteristics described in “draft-ietf-sip-callee-caps-01” [38] during IMS registration.

5.2.1a Implicit Registration

5.2.1a.0 General

When an user has a set of public user identities defined to be implicitly registered via single IMS registration of one of the public user identity’s in that set, it is considered to be an Implicit Registration. No single public identity shall be considered as a master to the other public user identities. Figure 5.2.1a shows a simple diagram of implicit registration and public user identities. In order to support this function, it is required that:

- HSS has the set of public user identities that are part of implicit registration.
- Cx reference point between S-CSCF and HSS shall support download of all public user identities associated with the implicit registration, during registration of any of the single public user identities within the set.
- All public user identities of an Implicit Registration set must be associated to the same private user identities. See figure 5.2.1.b for the detailed relationship between the public and private user entities within an Implicit Registration set.
- When one of the public user identities within the set is registered, all Public user identities associated with the implicit registration set are registered at the same time.
- When one of the public user identities within the set is de-registered, all public user identities that have been implicitly registered are de-registered at the same time.
- Registration and de-registration always relates to a particular contact address. A Public user identitity that has been registered (including when implicitly registered) with different contact addresses remains registered in relation to those contact addreses that have not been de-registered.
- Public user identities belonging to an implicit registration set may point to different service profiles; or some of these public user identities may point to the same service profile.
- When a public user identity belongs to an implicit registration set, it cannot be registered or de-registered individually without the public user identity being removed from the implicit registration list.
- All IMS related registration timers should apply to the set of implicitly registered public user identities

- S-CSCF, P-CSCF and UE shall be notified of the set of public user identities belonging to the implicitly registered function. Session set up shall not be allowed for the implicitly registered public user identities until the entities are updated, except for the explicitly registered public user identity.
- The S-CSCF shall store during registration all the Service profiles corresponding to the public user identities being registered.
- When a public user identity is barred from IMS communications, only the HSS and S-CSCF shall have access to this public user identity.

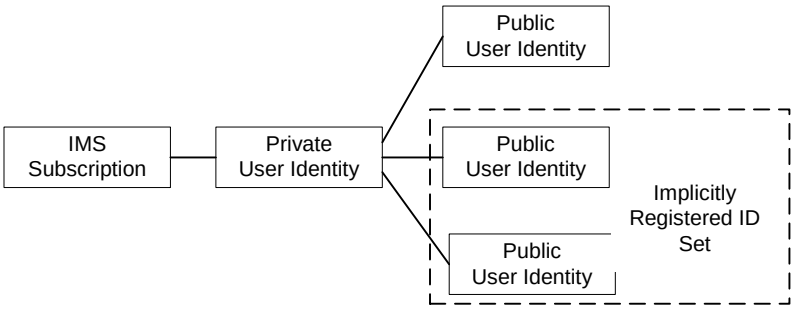


Figure 5.2.1a Relationship of public user identities when implicitly registered

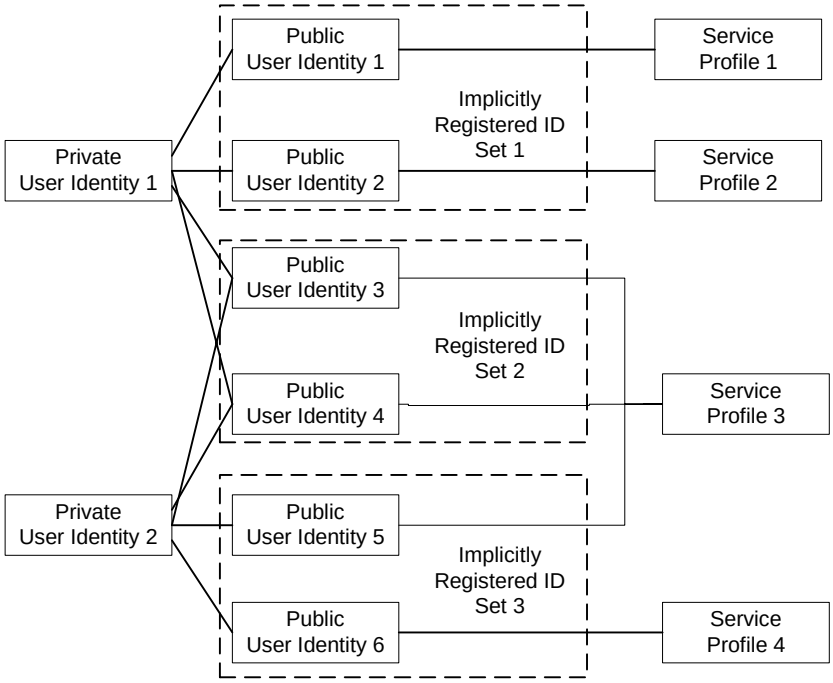


Figure 5.2.1.b – The relation of two shared Public User Identities (Public-ID-3 and 4) and Private User Identities

5.2.1a.1 Implicit Registration for UE without ISIM

In case an UE is registering in the IMS without ISIM, it shall require the network's assistance to register atleast one public user identity, which is used for session establishment & IMS signalling. Implicit registration shall be used as part of a mandatory function for these ISIM-less UEs to register the public user identity(s). In addition to the functions defined in section 5.2.1a, the following additional functions are required for this scenario.

- The Temporary public identity shall be used for initial registration process
- It shall be defined in HSS that if the user does not have implicit registration activated then the user shall not be allowed to register in the IMS using the Temporary public user identity.

**** Next Change ****

5.3.2 Network initiated de-registration

5.3.2.0 General

If an ungraceful session termination occurs (e.g. flat battery or mobile leaves coverage), when a stateful proxy server (such as the S-CSCF) is involved in a session, memory leaks and eventually server failure can occur due to hanging state machines. To ensure stable S-CSCF operation and carrier grade service, a mechanism to handle the ungraceful session termination issue is required. This mechanism should be at the SIP protocol level in order to guarantee access independence for the IM CN subsystem.

The IM CN subsystem can initiate a Network Initiated De-Registration procedures for the following reasons:

- Network Maintenance.
  Forced re-registrations from users, e.g. in case of data inconsistency at node failure, in case of UICC lost, etc. Cancelling the current contexts of the user spread among the IM CN Subsystem network nodes at registration, and imposing a new IM registration solves this condition.

- Network/traffic determined.
  The IM CN subsystem must support a mechanism to avoid duplicate registrations or inconsistent information storage. This case will occur when a user roams to a different network without de-registering the previous one. This case may occur at the change of the roaming agreement parameters between two operators, imposing new service conditions to roamers.

- Application Layer determined.
  The service capability offered by the IM CN Subsystem to the Application Layers may have parameters specifying whether all IM CN subsystem registrations are to be removed, or only those from one or a group of terminals from the user, etc.

- Subscription Management
  The operator must be able to restrict user access to the IM CN subsystem upon detection of contract expiration, removal of IM subscription, fraud detection, etc.In case of changes in service profile of the user, e.g. the user subscribes to new services, it may possible that new S-CSCF capabilities, which are required from the S-CSCF, are not supported by the current S-CSCF which has been assigned to the user. In this case, it shall be possible to actively change the S-CSCF by using the network initiated de-registration by HSS procedure.

The following sections provide scenarios showing SIP application de-registration. Note that these flows have avoided the strict use of specific SIP protocol message names. This is in an attempt to focus on the architectural aspects rather than the protocol.

Two types of network-initiated de-registration procedures are required:

- To deal with registrations expirations.

- To allow the network to force de-registrations following any of the approved possible causes for this to occur.

5.3.2.1 Network Initiated Application (SIP) De-registration, Registration Timeout

The following flow shows a network initiated IM CN subsystem terminal application (SIP) de-registration based on a registration timeout. A timer value is provided at initial registration and is refreshed by subsequent re-registrations. The flow assumes that the timer has expired. The locations (home or visited network) of the P-CSCF and S-CSCF are not indicated as the scenario remains the same for all cases.

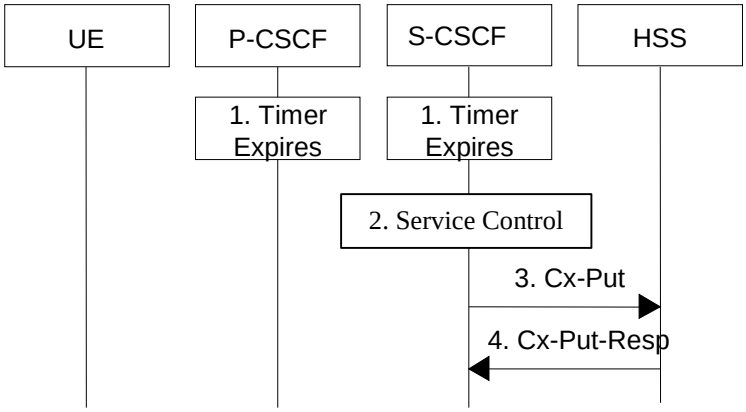


Figure 5.4: Network initiated application de-registration, registration timeout

1. The registration timers in the P-CSCF and in the S-CSCF expire. The timers are assumed to be close enough that no external synchronisation is required. The P-CSCF updates its internal databases to remove the public user identity from being registered. It is assumed that any cleanup of IP-Connectivity Access Network resources will be handled by independent means.

2. Based on the filter criteria, the S-CSCF shall send de-registration information to the service control platform and perform whatever service control procedures are appropriate. Service control platform removes all subscription information related to this specific public user identity.

3. Based on operator choice the S-CSCF can send either Cx-Put (public user identity, private user identity, clear S-CSCF name) or Cx-Put (public user identity, private user identity, keep S-CSCF name), and the public user identity is no longer considered registered in the S-CSCF. The HSS then either clears or keeps S-CSCF name for that public user identity according to the request. In both cases the state of the public user identity is stored as unregistered in the HSS. If the S-CSCF name is kept, then the HSS shall be able to clear the serving S-CSCF at any time.

4. The HSS shall send Cx-Put Resp to the S-CSCF to acknowledge the sending of Cx-Put.

5.3.2.2 Network Initiated Application (SIP) De-registration, Administrative

5.3.2.2.0 General

For different reasons (e.g., subscription termination, lost terminal, etc.) a home network administrative function may determine a need to clear a user's SIP registration. This function initiates the de-registration procedure and may reside in various elements depending on the exact reason for initiating the de-registration.

One such home network element is the HSS, which already knows the S-CSCF serving the user and that for this purpose makes use of the Cx-Deregister. Another home network element that could initiate the de-registration is the S-CSCF, in which case it makes use of the Cx-Put to inform the HSS. Other trusted/secured parties may also initiate de-registration to the S-CSCF.

The following flow shows a network initiated IM CN subsystem terminal application (SIP) de-registration based on an administrative action for example. The IP transport infrastructure is not notified. If complete packet access is to be denied, a transport layer administrative mechanism would be used. This scenario does not address the administrative mechanisms used for updating any subscriber records, EIR records, access authorisation, etc. This scenario only addresses the specific action of clearing the SIP application registration that is currently in effect.

As determined by the operator, on-going sessions may be released by using network initiated session release procedures in Section 5.10.3.

5.3.2.2.1 Network Initiated De-registration by HSS, administrative

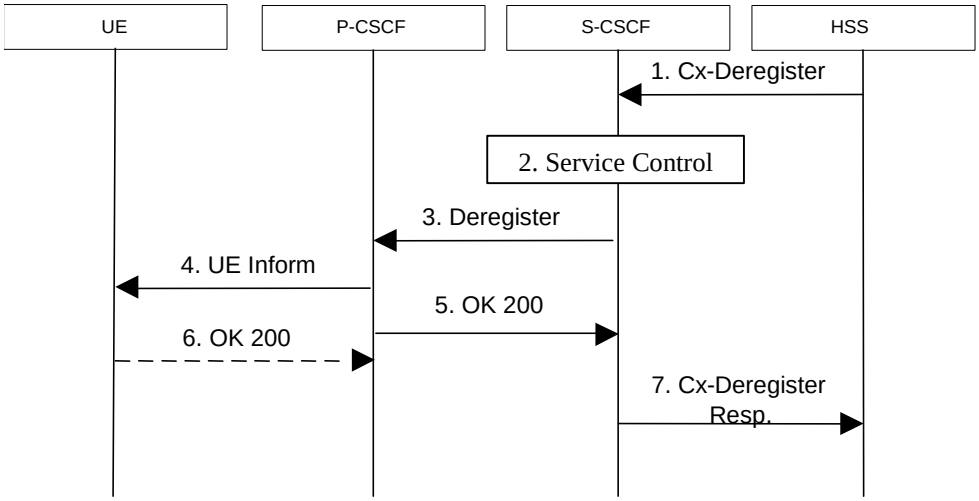


Figure 5.5: Network initiated application de-registration by HSS, administrative

1. HSS initiates the de-registration, sending a Cx-Deregister (user identity) which may include the reason for the de-registration.

2. Based on the filter criteria, the S-CSCF shall send de-registration information to the service control platform and perform whatever service control procedures are appropriate.

3. The S-CSCF issues a de-registration towards the P-CSCF for this user and updates its internal database to remove the user from being registered. The reason for the de-registration received from the HSS shall be included if available.

4. The P-CSCF informs the UE of the de-registration and without modification forwards the reason for the de-registration, if available. Due to loss of contact with the mobile, it might be possible that the UE does not receive the information of the de-registration.

5. The P-CSCF sends a response to the S-CSCF and updates its internal database to remove the user from being registered.

6. When possible, the UE sends a response to the P-CSCF to acknowledge the de-registration. A misbehaving UE or a UE that is out of P-CSCF coverage could not answer properly to the de-registration request. The P-CSCF should perform the de-registration in any case, e.g., after the timer for this request expires.

If the UE does not perform automatic re-registration due to the de-registration the user shall be informed about the de-registration and of the reason, if available.

Note: Steps 4 and 5 may be done in parallel: the P-CSCF does not wait for an answer from the UE before answering to the S-CSCF

7. The S-CSCF returns a response to the entity that initiated the process.

Note: Another trusted/secured party may also request for de-registration via HSS through administrative mechanisms provided by the operator.

5.3.2.2.2 Network Initiated De-registration by S-CSCF

A service platform may determine a need to clear a user's SIP registration. This function initiates the de-registration procedure and resides in a service platform.

The following flow shows a service control initiated IMS terminal application (SIP) de-registration. The IP transport infrastructure is not notified. If complete packet access is to be denied, a transport layer administrative mechanism would be used. This scenario does not address the administrative mechanisms used for updating any subscriber records, EIR records, access authorisation, etc. This scenario only addresses the specific action of clearing the SIP application registration that is currently in effect.

As determined by the operator, on-going sessions may be released by using network initiated session release procedures in Section 5.10.3.

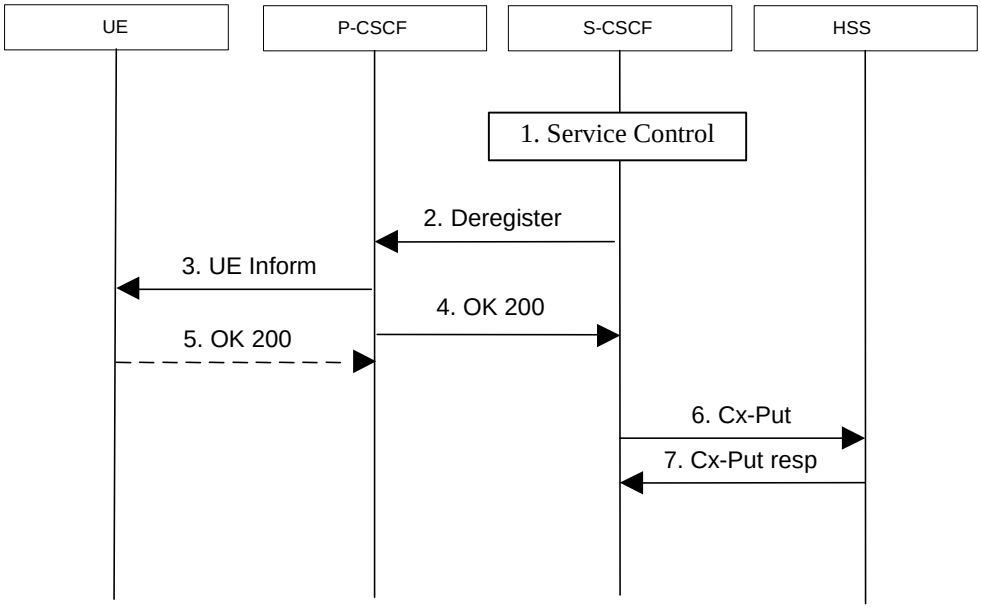


Figure 5.5a: Network initiated application de-registration, service platform

1. The S-CSCF receives de-registration information from the service platform and invokes whatever service logic procedures are appropriate. This information may include the reason for the de-registration.

2. The S-CSCF issues a de-registration towards the P-CSCF for this user and updates its internal database to remove the user from being registered. The reason for the de-registration shall be included, if available.

3. The P-CSCF informs the UE of the de-registration, and without modification forwards the reason for the de-registration, if available. Due to loss of contact with the mobile, it might be possible that the UE does not receive the information of the de registration.

4. The P-CSCF sends a response to the S-CSCF and updates its internal database to remove the user from being registered.

5. When possible, the UE sends a response to the P-CSCF to acknowledge the de-registration. A misbehaving UE or a UE that is out of P-CSCF coverage could not answer properly to the de-registration request. The P-CSCF should perform the de-registration in any case, e.g., after the timer for this request expires.

   If the UE does not perform automatic re-registration due to the de-registration the user shall be informed about the de-registration and of the reason, if available.

Note: Steps 4 and 5 may be done in parallel: the P-CSCF does not wait for an answer from the UE before answering to the S-CSCF

6. The S-CSCF sends an update to the HSS to remove itself as the registered S-CSCF for this user.

7. The HSS confirms the update.

Note: Another trusted/secured party may also initiate the de-registration, for example, by issuing a third party SIP registration with timer set to 0 via S-CSCF.

5.4 Procedures for IP multi-media sessions

5.4.0 General

Basic IMS sessions between mobile users will always involve two S-CSCFs (one S-CSCF for each). The session flow is decomposed into two parts: an origination part between the UE & the S-CSCF and termination part between the S-CSCF and the UE, including all network elements in the path.

A basic session between a user and a PSTN endpoint involves an S-CSCF for the UE, a BGCF to select the PSTN gateway, and an MGCF for the PSTN.

The session flow is decomposed into three parts – an origination part, an inter-Serving-CSCF/ MGCF part, and a termination part. The origination part covers all network elements between the UE (or PSTN) and the S-CSCF for that UE (or MGCF serving the MGW). The termination part covers all network elements between the S-CSCF for the UE (or MGCF serving the MGW) and the UE (or PSTN).

5.4.1 Bearer interworking concepts

Voice bearers from the IM CN subsystem need to be connected with the voice bearers of other networks. Elements such as Media Gateway Functions (MGW) are provided to support such bearer interworking. One of the functions of the MGW may be to support transcoding between a codec used by the UE in the IM CN subsystem and the codec being used in the network of the other party.

Default codecs to be supported within the UE are defined in [21]. The use of default codecs within the UE enables the IM CN subsystem to interwork with other networks on an end to end basis or through transcoding.

The IM CN subsystem is also able to interwork with the CS networks (e.g. PSTN, ISDN, CS domain of some PLMN) by supporting, for example, AMR to G.711 [17] transcoding in the IMS MGW element. Furthermore to allow interworking between users of the IM CN subsystem and IP multimedia fixed terminals and other codecs may (this is implementation dependent) be supported by the MGW.

In order to support existing network capabilities, it is required that a UE be able to send DTMF tone indications to the terminating end of a session using the bearer, i.e. inband signalling. An additional element for bearer interworking is the interworking of these DTMF tones between one network and another. This may involve the generation of tones on the bearer of one network based on out of band signaling on the other network. In such a case, the MGW shall provide the tone generation under the control of the MGCF.

**** Next Change ****

5.4.6 End-user preferences and terminal capabilities

5.4.6.0 General

Due to different capabilities of the originating and terminating terminals, it might not be possible to establish all the media suggested by the originator for a particular session. In addition, the destination user may have different preferences of type of media depending on who is originating and on the situation e.g. being in a meeting or driving the car etc.

5.4.6.1 Objectives

The general objectives concerning terminal capabilities and end-user behaviour are listed below.

- The capabilities of the terminal have impact on the SDP description in the SIP session flows, since different terminals may support different media types (such as video, audio, application or data) and may have implemented different set of codecs for audio and video. Note that the capabilities of the terminal may change when an external device, such as a video camera is attached to the terminal.

- The configuration of the terminal changes the capabilities of the terminal. This can be done by attaching external devices or possibly by a user setting of certain parameters or profiles in the terminal.

- The preferences of the destination user may depend on who is originating the session and on the situation. Cost, associated with the session, may also be another factor, i.e. depending on time of the day or day of the week etc. Due to this reason the user may want to accept or reject certain media components.

- The available resources in the network play an important role, as certain media streams, consuming high bandwidth, may be denied. Therefore, before the user is alerted that the session set up is successful, it is

assumed that the network has guaranteed and has reserved the needed resources for one or several media streams of the session. This does not preclude the possibility for the user to indicate his/her preferences regarding the session also after the alerting, in which case the initial resource reservations may have to be modified.

- End-to-end quality of service may be provided by using a variety of mechanisms, including guaranteed end-to-end QoS and best effort. The network may not be able to guarantee the requested end-to-end QoS. This may be the case when the user is establishing sessions through the public Internet. On the other hand, certain sessions, with the agreement of the initiating and terminating endpoints, should have the right to go through even without having the requested QoS guarantee.

**** Next Change ****

5.4.7 Interaction between QoS and session signalling

5.4.7.0 General

At IP-CAN bearer activation the user shall have access to either IP-CAN services without service-based local policy, or IP-CAN services with service-based local policy. It is operator choice whether to offer both or only one of these alternatives for accessing the IM Subsystem.

When using IP-CAN without service-based local policy, the bearer is established according to the user's subscription, local operator's IP bearer resource based policy, local operator's admission control function and roaming agreements.

When using IP-CAN with service-based local policy, Service-Based Local Policy decisions (e.g., authorisation and control) are also applied to the bearer.

The description in this clause and the following sub-clauses (sub-clauses 5.4.7.1 – 5.4.7.7) is applicable for the case when service-based local policy is employed.

The IP-Connectivity Access Network contains a Policy Enforcement Function (PEF) that has the capability of policing packet flow into the IP network, and restricting the set of IP destinations that may be reached from/through an IP-CAN bearer according to a packet classifier. This service-based policy 'gate' function has an external control interface that allows it to be selectively 'opened' or 'closed' on the basis of IP destination address and port. When open, the gate allows packets to pass through (to the destination specified in the classifier) and when closed, no packets are allowed to pass through. The control is performed by a PDF, which is a logical entity of the P-CSCF. (Note: If the PDF is implemented in a separate physical node, the interface between the PDF and the P-CSCF is not standardised).

There are eight interactions defined for service-based local policy:

1. Authorize QoS Resources.
2. Resource Reservation with Service-based Local Policy.
3. Approval of QoS Commit for resources authorised in (1), e.g. 'open' the 'gate'.
4. Removal of QoS Commit for resources authorised in (1), e.g. 'close' the 'gate'.
5. Revoke Authorisation for IP-CAN and IP resources.
6. Indication of IP-CAN bearer release from the PEF in the IP-Connectivity Access Network to the PDF.
7. Authorization of IP-CAN bearer modification
8. Indication of IP-CAN bearer modification from the PEF in the IP-Connectivity Access Network to the PDF.

These requirements and functional description of these interactions are explained further in the following sections. The complete specification of the interface between the Policy Decision Function and the Policy Enforcement Function is contained in TS 23.207.

5.4.7.1 Authorize QoS Resources

The Authorize QoS Resources procedure is used during an establishment of a SIP session. The P-CSCF(PDF) shall use the SDP contained in the SIP signaling to calculate the proper authorisation. The PDF authorizes the required QoS resources.

The authorisation shall include binding information, which shall also be provided by the UE in the allocation request to the IP-CAN, which enables accurate matching of requests and authorisations. The binding information includes an Authorisation Token sent by the P-CSCF to the UE during SIP signaling, and one or more Flow Identifiers, which are used, by the UE, the PEF within the IP-Connectivity Access Networkand PDF to uniquely identify the media component(s). If forking has occurred, the P-CSCF will re-use the same Authorisation Token in all subsequent provisional responses belonging to the same session. If the least upper bound of the requested resources is changed due to a subsequently received response then an update of the authorised resources is performed.

The authorisation shall be expressed in terms of the IP resources to be authorised and shall include limits on IP packet flows, and may include restrictions on IP destination address and port.

**** Next Change ****

5.4.9 Event and information distribution

5.4.9.0 General

The S-CSCF and Application Servers (SIP-AS, IM-SSF, OSA-SCS) shall be able to send service information messages to endpoints. This shall be done based on a SIP Request/Response information exchange containing the service information and/or a list of URI(s) pointing to the location of information represented in other media formats. The stimulus for initiating the service event related information message may come from e.g. a service logic residing in an application server.

In addition, the end points shall also be able to send information to each other. This information shall be delivered using SIP based messages. The corresponding SIP messages shall be forwarded along the IMS SIP signalling path. This includes the S-CSCF but may also include SIP application servers. The information may be related or unrelated to any ongoing session and/or may be independent of any session. Applicable mechanisms (for e.g. routing, security, charging, etc) defined for IMS SIP sessions shall also be applied for the SIP based messages delivering the end-point information. The length of the information transferred is restricted by the message size (e.g. the MTU), so fragmentation and re-assembly of the information is not required to be supported in the UE. This information may include e.g. text message, http url, etc.

This mechanism considers the following issues:

- The IMS has the capability to handle different kinds of media. That is, it is possible to provide information contained within several different media formats e.g. text, pictures or video.

- The UE's level of supporting service event related information and its exchange may depend on the UE's capabilities and configuration.

- A UE not participating in the service related information exchange shall not be effected by a service related information exchange possibly being performed with another UE of the session.

Note: The service event related information exchange may either take place in the context of a session, or independently outside the context of any existing session.

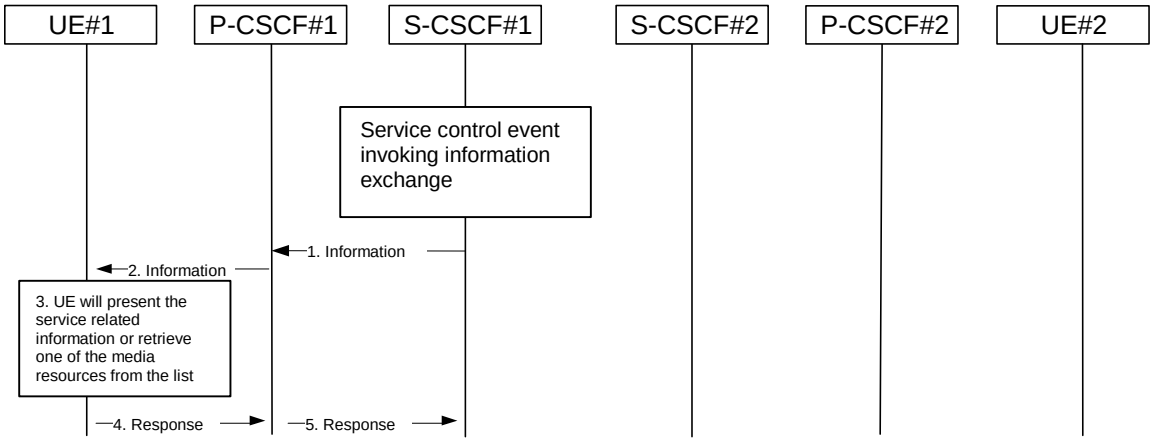


Figure 5.8: Providing service event related information to related endpoint

1. When a service event occurs that the S-CSCF or the Application Server wishes to inform an endpoint about, the S-CSCF or the Application Server generates a message request containing information to be presented to the user. The contents may include text describing the service event, a list of URI(s) or other service modification information.

2. P-CSCF forwards the message request.

3. UE presents the service-related information, to the extent that it conforms to its capabilities and configuration, to the user.

4. Possibly after interaction with the user, the UE will be able to include information in the response to the S-CSCF.

5. P-CSCF forwards the response.

Note 1: The UE may retrieve service event related information using IP-CAN or IMS procedures.

Note 2: transport aspects of the information transfer described above may require further considerations.

5.4.9.1 Subscription to event notifications

The SIP-event notification mechanism allows a SIP entity to request notification from remote nodes indicating that certain standardised events have occurred. Examples of such of events are changes in presence states, changes in registration states, changes in Subscription authorisation policies (see 3GPP TS 23.141 [36]) and other events that are caused by information changes in e.g. Application Servers or S-CSCF.

It shall be possible to either fetch relevant information once or monitor changes over a defined time. It shall be possible for a user to subscribe to events related to his/her own subscription (e.g. when the user subscribes to his own registration state) or to events related to other users' subscription (an example is when a watcher subscribes to presence information of a presentity, see 3GPP TS 23.141 [36]).

The S-CSCF is not mandated to stay in the path after the initial SubscribeEvent request and ACK has been exchanged, in case the S-CSCF does not execute any functions for the subsequent requests and responses of the dialog. The example, in figure 5.8a below, assumes that the S-CSCF does not want to execute any functions for the subsequent requests.

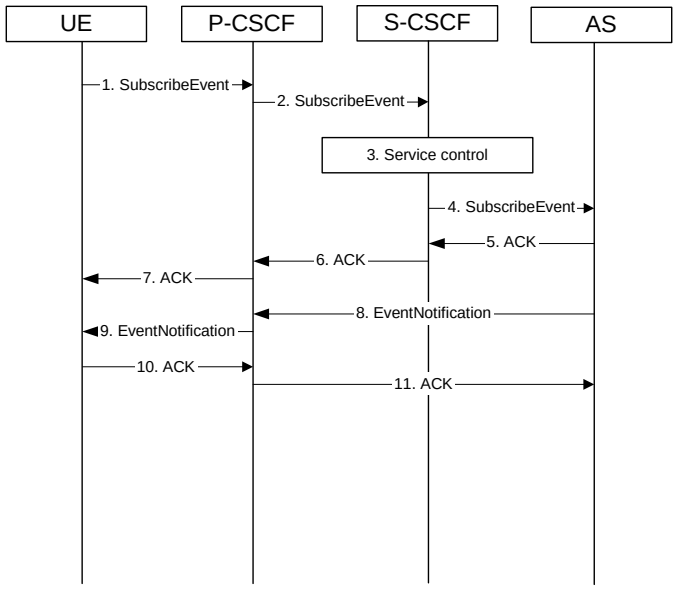


Figure 5.8a: Subscription to event in AS

1. The UE initiates a subscription to an AS requesting notification of any changes in specified information stored in the control of the AS
2. The P-CSCF remembers (from the registration process) the next hop CSCF for this UE, i.e., the SubscribeEvent is forwarded to the S-CSCF in the home network.
3. The S-CSCF invokes whatever service logic procedures are appropriate for this request.
4. The S-CSCF applies regular routing procedures and forwards the request to the next hop.
5. The AS acknowledges the SubscribeEvent request.
6. The S-CSCF forwards the acknowledgement to the P-CSCF.
7. The P-CSCF forwards the acknowledgement to the UE.
8. As soon as the AS sends an acknowledgement to accept the subscription, the AS sends an EventNotification message with the current information the UE subscribed to. The EventNotification is sent along the path set-up by the SubscribeEvent dialog to the P-CSCF allocated to the UE. Further notifications, if monitor of changes was requested, sent by the AS is sent along the same path.
9. The P-CSCF forwards the EventNotification to the UE.
10. The UE acknowledges the EventNotification.
11. The P-CSCF forwards the acknowledgement to the AS.

**** Next Change ****

5.4.12 Configuration and Routing principles for Public Service Identities

5.4.12.0 General

Depending on the service nature, different mechanisms may be used for configuration and routing of PSIs according to operator preference.

When PSIs are created, the uniqueness of a PSI shall be ensured. Note that only the username part of a PSI is definable within a predefined hostname(s).

Whenever possible, routing to/from a Public Service Identity (PSI) should be provided using basic principles used for IMS routing.

**** Next Change ****

5.5 Serving-CSCF/MGCF to serving-CSCF/MGCF procedures

5.5.0 General

This section presents the detailed application level flows to define the procedures for Serving-CSCF to Serving-CSCF.

This section contains four session flow procedures, showing variations on the signalling path between the Serving-CSCF that handles session origination, and the Serving-CSCF that handles session termination. This signalling path depends on:

- whether the originator and destination are served by the same network operator,

- whether the network operators have chosen to hide their internal configuration.

The Serving-CSCF handling session origination performs an analysis of the destination address, and determines whether it is a subscriber of the same network operator or a different operator.

If the analysis of the destination address determined that it belongs to a subscriber of a different operator, the request is forwarded (optionally through an I-CSCF(THIG) within the originating operator's network) to a well-known entry point in the destination operator's network, the I-CSCF. The I-CSCF queries the HSS for current location information. The I-CSCF then forwards the request to the S-CSCF. If the analysis of the destination address determines that it belongs to a subscriber of the same operator, the S-CSCF passes the request to a local I-CSCF, who queries the HSS for current location information. The I-CSCF then forwards the request to the S-CSCF.

5.5.1 (S-S#1) Different network operators performing origination and termination

The Serving-CSCF handling session origination performs an analysis of the destination address, and determines that it belongs to a subscriber of a different operator. The request is therefore forwarded (optionally through an an I-CSCF(THIG) within the originating operator's network) to a well-known entry point in the destination operator's network, the I-CSCF. The I-CSCF queries the HSS for current location information, and finds the user either located in the home service area, or roaming. The I-CSCF therefore forwards the request to the S-CSCF serving the destination user.

Origination sequences that share this common S-S procedure are:

MO#1 Mobile origination, roaming. The "Originating Network" of S-S#1 is therefore a visited network.

MO#2 Mobile origination, home. The "Originating Network" of S-S#1 is therefore the home network.

PSTN-O PSTN origination. The "Originating Network" of S-S#1 is the home network. The element labeled S-CSCF#1 is the MGCF of the PSTN-O procedure.

Termination sequences that share this common S-S procedure are:

MT#1 Mobile termination, roaming. The “Terminating Network” of S-S#1 is a visited network.

MT#2 Mobile termination, located in home service area. The “Terminating Network” of S-S#1 is the home network.

MT#3 Mobile termination, CS Domain roaming. The “Terminating Network” of S-S#1 is a CS domain network.

**** Next Change ****

5.6 Origination procedures

5.6.0 General

This section presents the detailed application level flows to define the Procedures for session originations.

The flows presented in the section assume the use of service-based local policy.

The session origination procedures specify the signalling path between the UE initiating a session setup attempt and the Serving-CSCF that is assigned to perform the session origination service. This signalling path is determined at the time of UE registration, and remains fixed for the life of the registration.

A UE always has a proxy (P-CSCF) associated with it. This P-CSCF performs resource authorisation, and may have additional functions in handling of emergency sessions. The P-CSCF is determined by the CSCF discovery process, described in Section 5.1.1 (Local CSCF Discovery).

As a result of the registration procedure, the P-CSCF determines the next hop toward the Serving-CSCF. This next hop is to the S-CSCF in the home network (possibly through an I-CSCF(THIG) to hide the network configuration) (MO#1). These next-hop addresses could be IPv6 addresses, or could be names that are translated via DNS to an IPv6 address.

Sessions originated in the PSTN to a mobile destination are a special case of the Origination procedures. The MGCF uses H.248 [19] to control a Media Gateway, and communicates with the SS7 network. The MGCF initiates the SIP request, and subsequent nodes consider the signalling as if it came from a S-CSCF.

5.6.1 (MO#1) Mobile origination, roaming

This origination procedure applies to roaming users.

The UE is located in a visited network, and determines the P-CSCF via the CSCF discovery procedure described in section 5.1.1. The home network advertises either the S-CSCF or an I-CSCF as the entry point from the visited network.

When registration is complete, P-CSCF knows the name/address of the next hop in the signalling path toward the serving-CSCF, either I-CSCF(THIG) (if the home network wanted to hide their internal configuration) or S-CSCF (if there was no desire to hide the network configuration). I-CSCF, if it exists in the signalling path, knows the name/address of S-CSCF.

**** Next Change ****

5.7 Termination procedures

5.7.0 General

This section presents the detailed application level flows to define the Procedures for session terminations.

The flows presented in the section assume the use of service-based local policy.

The session termination procedures specify the signalling path between the Serving-CSCF assigned to perform the session termination service and the UE. This signalling path is determined at the time of UE registration, and remains fixed for the life of the registration.

A UE always has a proxy (P-CSCF) associated with it. This P-CSCF performs resource authorisation for the sessions to the UE. The P-CSCF is determined by the CSCF discovery process, described in Section 5.1.1 (Local CSCF Discovery).

As a result of the registration procedure, the P-CSCF knows the address of the UE. The assigned S-CSCF, knows the name/address of the P-CSCF (procedure MT#3, and MT#4, depending on the location of S-CSCF and P-CSCF). If the network operator owning the S-CSCF wants to keep their configuration private, the S-CSCF will have chosen an I-CSCF(THIG) who will perform the configuration hiding and pass messages to the P-CSCF (procedure MT#1).

Sessions destined to the PSTN are a special case of the Termination procedures. The MGCF uses H.248 to control a Media Gateway, and communicates with the SS7 network. The MGCF receives and processes SIP requests, and subsequent nodes consider the signalling as if it came from a S-CSCF.

5.7.1 (MT#1) Mobile termination, roaming

This termination procedure applies to roaming users.

The UE is located in a visited network, and determines the P-CSCF via the CSCF discovery procedure described in section 5.1.1. The home network advertises either the S-CSCF, or an I-CSCF(THIG), as the entry point from the visited network.

When registration is complete, S-CSCF knows the name/address of its next hop in the signalling path, either I-CSCF or P-CSCF, I-CSCF (if it exists) knows the name/address of P-CSCF, and P-CSCF knows the name/address of the UE.

**** Next Change ****

5.8 Procedures related to routing information interrogation

5.8.0 General

When a mobile terminated session set-up arrives at an I-CSCF that is authorised to route sessions, the I-CSCF interrogates the HSS for routing information. The mobile terminated sessions for a user shall be routed to a S-CSCF.

The Cx reference point shall support retrieval of routing information from HSS to I-CSCF. The resulting routing information is the contact information of S-CSCF.

5.8.1 User identity to HSS resolution

This section describes the resolution mechanism, which enables the I-CSCF, the S-CSCF and the AS to find the address of the HSS, that holds the subscriber data for a given user identity when multiple and separately addressable HSSs have been deployed by the network operator. This resolution mechanism is not required in networks that utilise a single HSS e.g. optionally, it could be switched off on the I-CSCF and on the S-CSCF and/or on the AS using O&M mechanisms. An example for a single HSS solution is a server farm architecture. By default, the resolution mechanism shall be supported.

On REGISTER and on MT INVITEs, the I-CSCF queries the HSS for user's subscription specific data, e. g. the actual location or authentication parameters. This also has to be accomplished by the S-CSCF on REGISTER. In the case when more than one independently addressable HSS is utilized by a network operator, the HSS where user information for a given subscriber is available has to be found. To get the HSS name the I-CSCF and the S-CSCF query the Subscription Locator Functional (SLF) entity.

The subscription locator is accessed via the Dx interface or via the Dh interface. The Dx interface is the standard interface between the CSCF and the SLF and the Dh interface is the standard interface between the AS and the SLF. The synchronisation between the SLF and the different HSSs is an O&M issue.

A way to use the subscription locator is described in the following.

The Dx interface provides:

- an operation to query the subscription locator from the I-CSCF or from the S-CSCF, respectively
- a response to provide the HSS name towards the I-CSCF or towards the S-CSCF, respectively.

By sending the Dx-operation DX_SLF_QUERY the I-CSCF or the S-CSCF indicates a user identity of which it is looking for an HSS. By the Dx-operation DX_SLF_RESP the SLF responds with the HSS name. The I-CSCF or the S-CSCF, respectively, continues by querying the selected HSS. As an option at the registration flow, the I-CSCF may forward the HSS name towards the serving CSCF to simplify the procedure by which the serving CSCF finds the subscriber's HSS. This option can be used in a single HSS environment.

Subclause 5.8.2 presents the session flows on REGISTER and subclause 5.8.3 on INVITE messages.

The Dh interface provides:

- an operation to query the subscription locator from the AS
- a response to provide the HSS name towards the AS.

By sending the Dh-operation DH_SLF_QUERY the AS indicates a public user identity of which it is looking for an HSS. By the Dh-operation DH_SLF_RESP the SLF responds with the HSS name. The AS continues by querying the selected HSS. The AS may store the HSS name for the subsequent Sh-operations.

Subclause 5.8.4 presents the message flow on the Dh interface.

**** Next Change ****

5.10 Session release procedures

5.10.0 General

This section provides scenarios showing SIP application session release. Note that these flows have avoided the strict use of specific SIP protocol message names. This is in an attempt to focus on the architectural aspects rather than the protocol. SIP is assumed to be the protocol used in these flows.

The session release procedures are necessary to ensure that the appropriate billing information is captured and to reduce the opportunity for theft of service by confirming that the bearers associated with a particular SIP session are deleted at the same time as the SIP control signalling and vice versa. Session release is specified for the following situations;

- Normal session termination resulting from an end user requesting termination of the session using session control signalling or deletion of the IP bearers associated with a session,
- Session termination resulting from network operator intervention,
- Loss of the session control bearer or IP bearer for the transport of the IMS signalling, and
- Loss of one or more radio connections which are used to transport the IMS signalling

As a design principle the session release procedures shall have a high degree of commonality in all situations to avoid complicating the implementation.

5.10.1 Mobile terminal initiated session release

The following flow shows a mobile terminal initiated IM CN subsystem application (SIP) session release. It is assumed that the session is active and that the bearer was established directly between the two visited networks (the visited networks could be the Home network in either or both cases). Furthermore, the flow also assumes that service-based local policy is in use.

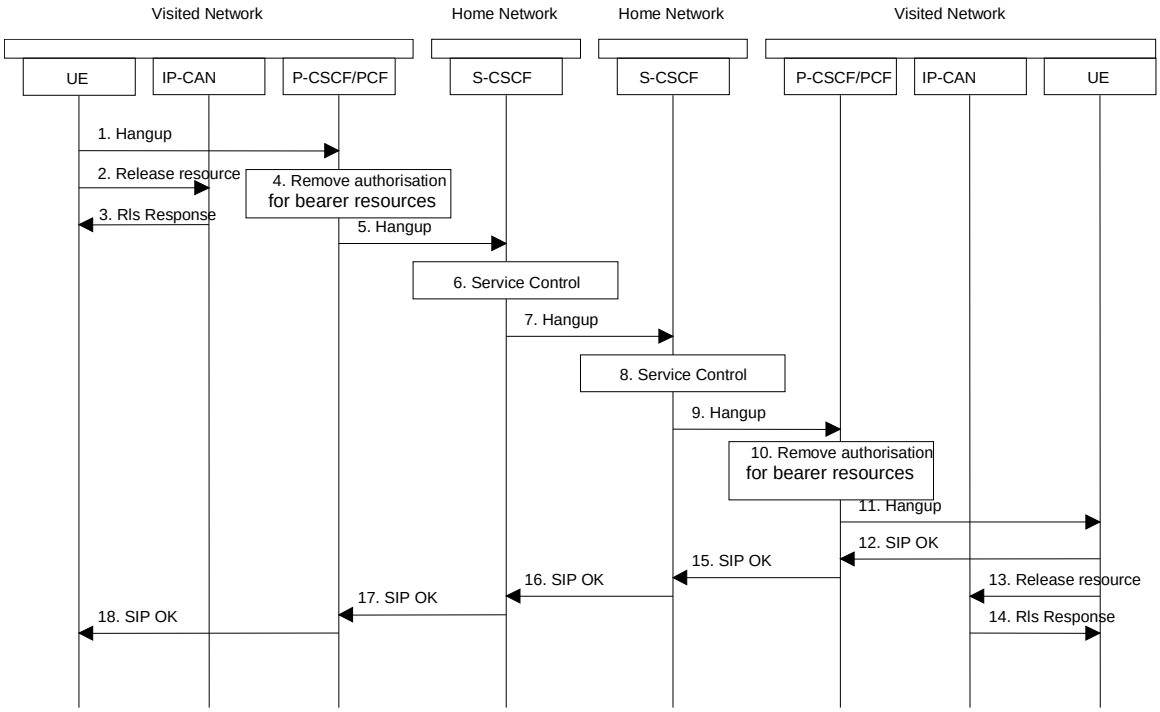


Figure 5.22: Mobile initiated session release

1. One mobile party hangs up, which generates a message (Bye message in SIP) from the UE to the P-CSCF.
2. Steps 2 and 3 may take place before or after Step 1 and in parallel with Step 4. The UE initiates the release of the IP-CAN bearer . The IP-CANreleases the IP-CAN bearer. The IP network resources that had been reserved for the message receive path to the mobile for this session are now released. This is initiated from the IP-CAN. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would invoked here.
3. The IP-CAN responds to the UE's bearer release request.
4. The P-CSCF/PDF removes the authorisation for resources that had previously been issued for this endpoint for this session. This step will also result in a release indication to the IP-CAN to confirm that the IP bearers associated with the session have been deleted
5. The P-CSCF sends a hangup to the S-CSCF of the releasing party.
6. The S-CSCF invokes whatever service logic procedures are appropriate for this ending session.
7. The S-CSCF of the releasing party forwards the Hangup to the S-CSCF of the other party.
8. The S-CSCF invokes whatever service logic procedures are appropriate for this ending session.
9. The S-CSCF of the other party forwards the Hangup on to the P-CSCF.
10. The P-CSCF/PDF removes the authorisation for resources that had previously been issued for this endpoint for this session. This step also results in a release indication to the IP-CAN to confirm that the IP bearers associated with the UE#2 session have been deleted.
11. The P-CSCF forwards the Hangup on to the UE.

12. The mobile responds with an acknowledgement, the SIP OK message (number 200), that is sent back to the P-CSCF.
13. Steps 13 and 14 may be done in parallel with step 12. The UE initiates the release of the IP-CAN bearer .
14. The IP-CAN releases the IP-CAN bearer. The IP network resources that were reserved for the message receive path to the mobile for this session are now released. This is initiated from the IP-CAN. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would invoked here.
15. The SIP OK message is sent to the S-CSCF.
16. The S-CSCF of the other party forwards the OK to the S-CSCF of the releasing.
17. The S-CSCF of the releasing party forwards the OK to the P-CSCF of the releasing.
18. The P-CSCF of the releasing party forwards the OK to the UE.

**** Next Change ****

5.10.3.1 Network initiated session release - P-CSCF initiated

5.10.3.1.0 General

This clause assumes that service-based local policy is applied

The following flows show a Network initiated IM CN subsystem application (SIP) session release. It is assumed that the session is active and that the bearer was established directly between the two visited networks (the visited networks could be the Home network in either or both cases).

A bearer is removed e.g. triggered by a UE power down, due to a previous loss of coverage, or accidental/malicious removal, etc. In this case the 'Indication of IP-CAN bearer release' procedure will be performed (see 3GPP TS 23.207). The flow for this case is shown in Figure 5.26.

Other network initiated session release scenarios are of course possible.

5.10.3.1.1 Network initiated session release - P-CSCF initiated – after removal of IP-Connectivity Access Network bearer

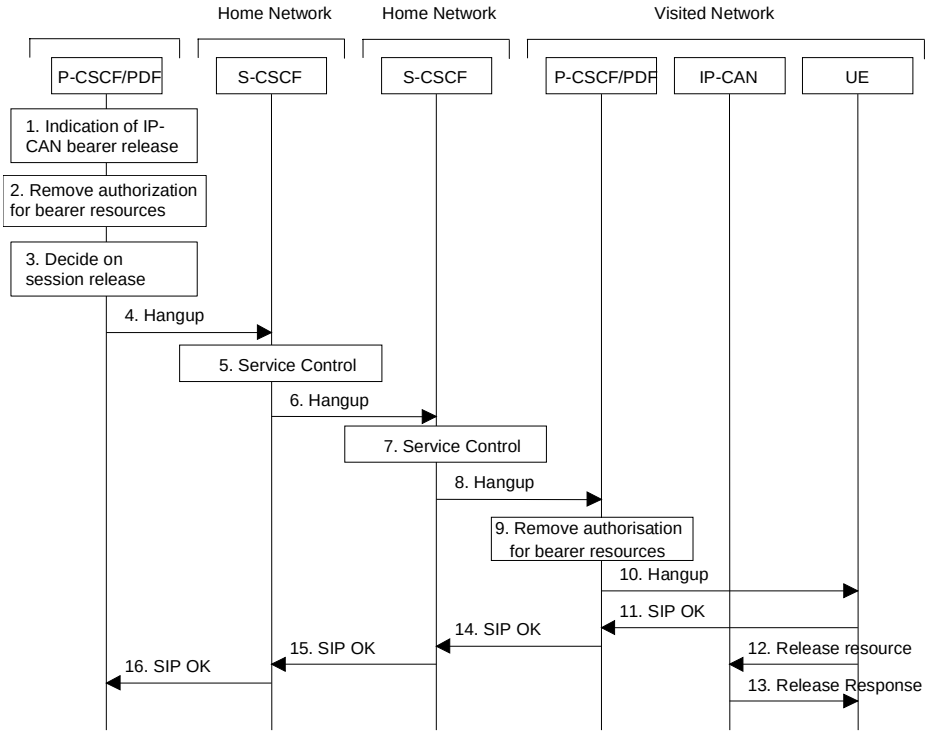


Figure 5.26: Network initiated session release - P-CSCF initiated – after removal of IP-CAN bearer

1. A bearer related to the session is terminated. The P-CSCF/PDF receives an indication of IP-CAN bearer release.

2. The P-CSCF/PDF removes the authorisation for resources related to the released bearer that had previously been issued for this endpoint for this session. It is optional for the P-CSCF/PDF to deactivate additional IP-CAN bearers (e.g. an IP-CAN bearer for chat could still be allowed). For these IP-CAN bearers the P-CSCF/PDF performs the 'Revoke Authorization for IP-CAN and IP Resources' procedure (see 3GPP TS 23.207).

3. The P-CSCF decides on the termination of the session. For example, the P-CSCF may decide to terminate the session if all IP-CAN bearers related to the same IMS session are deleted. If the P-CSCF decides to terminate the session then the P-CSCF/PDF removes the authorisation for resources that has previously been issued for this endpoint for this session. The P-CSCF/PDF shall perform the 'Revoke Authorization for IP-CAN and IP Resources' procedure (see 3GPP TS 23.207) in case that all IP-CAN bearers associated with the session have not been deleted yet.

The following steps are only performed in case the P-CSCF/PDF has decided to terminate the session.

4. The P-CSCF generates a Hangup (Bye message in SIP) to the S-CSCF of the releasing party.

5. The S-CSCF invokes whatever service logic procedures are appropriate for this ending session.

6. The S-CSCF of the releasing party forwards the Hangup to the S-CSCF of the other party.

7. The S-CSCF invokes whatever service logic procedures are appropriate for this ending session.

8. The S-CSCF of the other party forwards the Hangup on to the P-CSCF.

9. The P-CSCF/PDF removes the authorisation for resources that had previously been issued for this endpoint for this session. This step also results in a release indication to the IP-CAN to confirm that the IP bearers associated with the session have been deleted for UE#2.

10. The P-CSCF forwards the Hangup on to the UE.

11. The UE responds with an acknowledgement, the SIP OK message (number 200), which is sent back to the P-CSCF.

12. Steps 12 and 13 may be done in parallel with step 11. The UE initiates the release of the IP-CAN bearer .
13. The IP-CAN releases the IP-CAN bearer. The IP network resources that had been reserved for the message receive path to the UE for this session are now released. This is initiated from the IP-CAN. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would invoked here.
14. The SIP OK message is sent to the S-CSCF.
15. The S-CSCF of the other party forwards the OK to the S-CSCF of the releasing party.
16. The S-CSCF of the releasing party forwards the OK to the P-CSCF of the releasing party.

5.10.3.1.2 Void

**** Next Change ****

5.11.1 Session Hold and Resume Procedures

5.11.1.0 General

This section gives information flows for the procedures for placing sessions on hold that were previously established by the mechanisms of sections 5.4, 5.5, 5.6, and 5.7, and resuming the session afterwards. Two cases are presented: mobile-to-mobile (UE-UE), and a UE-initiated hold of a UE-PSTN session.

For a multi-media session, it shall be possible to place a subset of the media streams on hold while maintaining the others.

These procedures do not show the use of optional I-CSCFs. If an I-CSCF was included in the signalling path during the session establishment procedure, it would continue to be used in any subsequent flows such as the ones described in this section.

5.11.1.1 Mobile-to-Mobile Session Hold and Resume Procedures

An IMS session was previously established between an initiating UE and a terminating UE. Each of these UEs has an associated P-CSCF, and a S-CSCF assigned in their home network. The procedures are independent of whether the P-CSCFs are located in the home or visited networks. Therefore there is no distinction in this section of home network vs. visited network.

The hold and resume procedures are identical whether the UE that initiated the session also initiates the session-hold, or whether the UE that terminated the session initiates the session-hold.

When a media stream has been placed on hold, it shall not be resumed by any endpoint other than the one that placed it on hold.

The procedures for placing a media stream on hold, and later resuming the media stream, are as shown in the following information flow:

**** Next Change ****

5.11.2 Procedures for anonymous session establishment

5.11.2.0 General

This section gives information flows for the procedures for an anonymous session. However, sessions are not intended to be anonymous to the originating or terminating network operators.

The purpose of the mechanism is to give an IMS user the possibility to withhold certain identity information as specified in [39] and [40].

The privacy mechanism for IMS networks shall not create states in the CSCFs other than the normal SIP states.

IMS entities shall determine whether they are communicating with an element of the same Trust Domain for Asserted Identity or not as described in [40].

5.11.2.1 Signalling requirements for anonymous session establishment

The user shall be able to request that her identity information is not revealed to the terminating party.

If the originating user requests the session to be anonymous, the terminating side must not reveal any identity or signalling routing information to the destination endpoint. The terminating network should distinguish at least two cases, first where the originator intended the session to be anonymous, and second where the originator's identity was deleted by a transit network.

5.11.2.2 Bearer path requirements for anonymous session establishment

Procedures for establishment of an anonymous bearer path are not standardised in this release.

5.11.3 Procedures for codec and media characteristics flow negotiations

5.11.3.0 General

This section gives information flows for:

- the procedures for determining the set of negotiated characteritics between the endpoints of a multi-media session, determining the initial media characteristics (including common codecs) to be used for the multi-media session, and
- the procedures for modifying a session within the existing resources reservation or with a new resources reservation (adding/deleting a media flow, changing media characteristics including codecs, changing bandwidth requirements) when the session is already established.

5.11.3.1 Codec and media characteristics flow negotiation during initial session establishment

Initial session establishment in the IM CN subsystem must determine a negotiated set of media characteristics (including a common codec or set of common codecs for multi-media sessions) that will be used for the session. This is done through an end-to-end message exchange to determine the complete set of media characteristics, then the decision is made by the session initiator as to the initial set of media flows.

The session initiator includes an SDP in the SIP INVITE message that lists every media characteristics (including codecs) that the originator is willing to support for this session. When the message arrives at the destination endpoint, it responds with the media characteristics (e.g. common subset of codecs) that it is also willing to support for the session. Media authorisation is performed for these media characteristics. The session initiator, upon receiving the common subset, determines the media characteristics (including codecs) to be used initially.

The negotiation may take multiple media offered and answered between the end points until the media set is agreed upon.

Once the session is established, the procedures of section 5.11.3.2 may be used by either endpoint to change to a different media characteristic (e.g. codec) that was included in the initial session description, and for which no

additional resources are required for media transport. The procedures of section 5.11.3.3 may be used by either endpoint to change the session, which requires resources beyond those allocated to the existing session.

The flow presented here assumes that service-based local policy is in use.

**** Next Change ****

5.11.4 Procedures for providing or blocking identity

5.11.4.0 General

Identity is composed of a public user identity and an optional display name:

- The public user identity is used by any user for requesting communications to other users (see section 4.3.3.2).
- The display name is the user's name if available, an indication of privacy or unavailability otherwise. The display name is a text string which may identify the subscriber, the user or the terminal.

This section gives information flows for the procedures for providing the authenticated public user identity and the optional display Name information of the originating party to theterminating party. It also describes the mechanisms for blocking the display of public user identity and optional display name if requested by the originating party.

5.11.4.1 Procedures for providing the authenticated identity of the originating party

Authentication of the subscriber is performed during the registration procedures, as described in section 5.2.2.3. As a result of the registration procedures, one or several public user identity(ies) of the originating party is/are stored in P-CSCF#1. This is shown in the sub-procedure represented in the following information flow in step 1.

When UE#1 attempts to initiate a new session, it includes a public user identity in the INVITE request. P-CSCF#1 verifies that it is present and correct before passing the request to S-CSCF#1.

In the following call flow, it is assumed that no privacy has been required by UE#1.If thepublic user identity supplied by UE#1 in the INVITE request is incorrect, the P-CSCF may reject the request, or may overwrite with the correct URL.

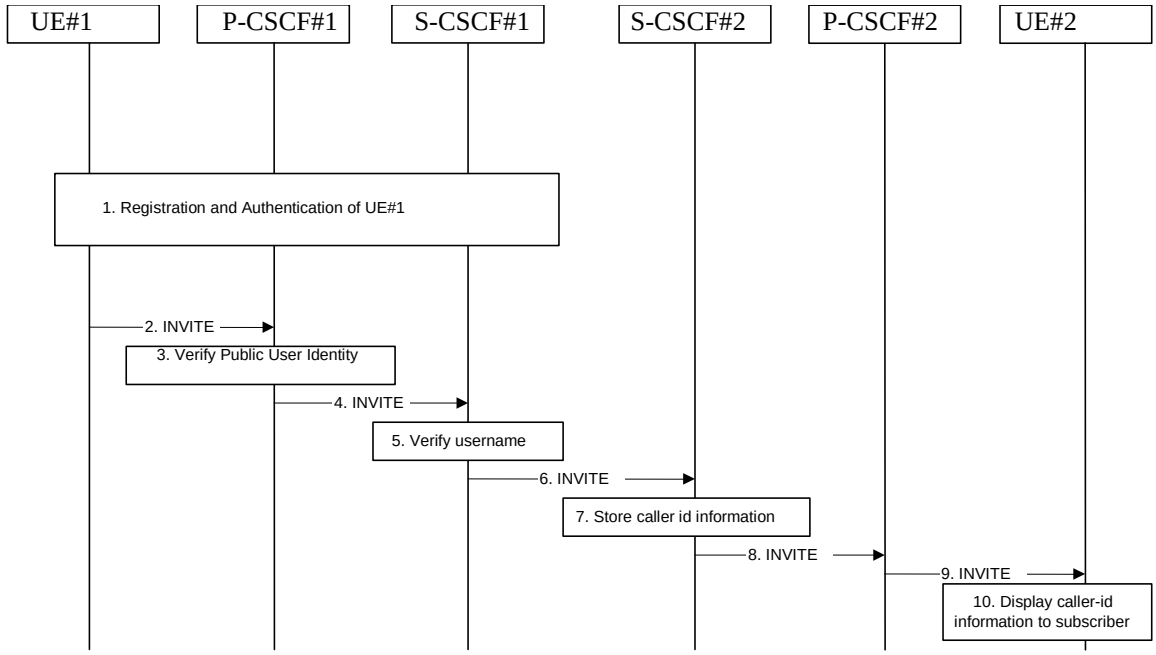


Figure 5.34: Providing the authenticated Identity of the originating party

The detailed procedure is as follows:

1. Registration and authentication of UE#1 is performed.
2. UE#1 initiates a new multi-media session, by sending an INVITE request to P-CSCF#1. This INVITE request includes a public user identity, and may include a display name that may identify the specific person using the UE.
3. P-CSCF#1 checks the public user identity of the originating party, and replaces it (or rejects the request) if it is incorrect.
4. P-CSCF#1 forwards the INVITE request, with the verified public user identity , to S-CSCF#1.
5. S-CSCF#1 invokes whatever service logic is appropriate for this session set up attempt to check in particular that no identity restriction is active.
6. S-CSCF#1 forwards the INVITE request, with verified public user identity and display name of the originting party if present, to S-CSCF#2.
8. S-CSCF#2 forwards the INVITE request to P-CSCF#2.
9. P-CSCF#2 forwards the INVITE request to UE#2.
10. UE#2 displays the public user identity and the display name information (i.e. user-name if available, indication of privacy or unavailability otherwise) to the terminating party.

**** Next Change ****

5.11.5 Session Redirection Procedures

5.11.5.0 General

This section gives information flows for the procedures for performing session redirection. The decision to redirect a session to a different destination may be made for different reasons by a number of different functional elements, and at different points in the establishment of the session.

Three cases of session redirection prior to bearer establishment are presented, and one case of session redirection after bearer establishment.

These cases enable the typical services of “Session Forward Unconditional”, “Session Forward Busy”, “Session Forward Variable”, “Selective Session Forwarding”, and “Session Forward No Answer”, though it is important to recognise that the implementation is significantly different from the counterparts in the CS domain.

5.11.5.1 Session Redirection initiated by S-CSCF to IMS

One of the functional elements in a basic session flow that may initiate a redirection is the S-CSCF of the destination user. The user profile information obtained from the HSS by the ‘Cx-pull’ during registration may contain complex logic and triggers causing session redirection. S-CSCF#2 sends the SIP INVITE request to the I-CSCF for the new destination (I-CSCF#F in the diagram), who forwards it to S-CSCF#F, who forwards it to the new destination.

In cases when the destination user is not currently registered in the IM CN subsystem, the I-CSCF may assign a temporary S-CSCF to invoke the service logic on behalf of the intended destination. This temporary S-CSCF takes the role of S-CSCF#2 in the following information flow.

The service implemented by this information flow is typically “Session Forward Unconditional”, “Session Forward Variable” or “Selective Session Forwarding”. S-CSCF#2 may also make use of knowledge of current sessions in progress at the UE, and implement “Session Forwarding Busy” in this way.

This is shown in the following information flow:

**** Next Change ****

5.11.6 Session Transfer Procedures

5.11.6.0 General

This section gives information flows for the procedures for performing session transfers. This is presented in two steps: first a basic primitive that can be used by endpoints to cause a multi-media session to be transferred, and second the procedures by which this primitive can be used to implement some well-known session-transfer services.

5.11.6.1 Refer operation

The refer primitive is an information flow indicating a “Refer” operation, which includes a component element “Refer-To” and a component element “Referred-By”. An information flow illustrating this is as follows:

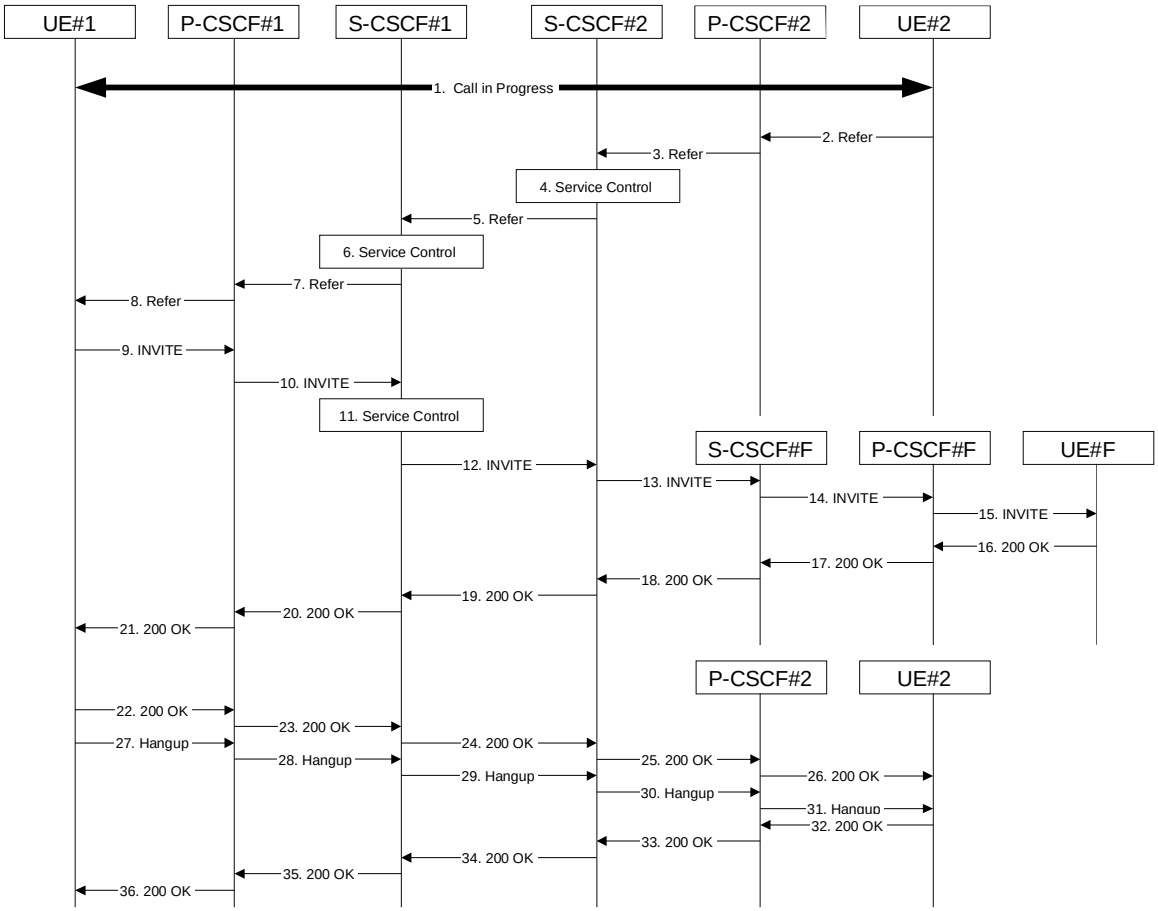


Figure 5.42: Refer operation

Step-by-step description of the information flow:

1. A multi-media session is assumed to already exist between UE#1 and UE#2, established either as a basic session or by one of the supplemental services described in this section.
2. UE#2 sends the Refer command to P-CSCF#2, containing “Refer-To” UE#F and “Referred-By” UE#2.
3. P-CSCF#2 forwards the message to S-CSCF#2

4. S-CSCF#2 invokes whatever service logic is appropriate for this request. If UE#2 does not subscribe to a transfer service, the request is rejected. S-CSCF#2 generates a private URL, addressed to itself, with the new destination informationand the billing information that will be needed for the new session. It replaces the “Refer-To” value in the request with the private URL.

5. S-CSCF#2 forwards the updated message to S-CSCF#1

6. S-CSCF#1 invokes whatever service logic is appropriate for this request. It stores the “Refer-To” and “Referred-By” information and replaces it with private URLs, so that UE#1 will not know the identity of UE#2 or UE#F.

7. S-CSCF#1 forwards the updated message to P-CSCF#1

8. P-CSCF#1 forwards the message to UE#1

9. UE#1 initiates a new multi-media session to the destination given by the “Refer-To”, which is a private URL pointing to S-CSCF#1.

10. P-CSCF#1 forwards the INVITE request to S-CSCF#1

11. S-CSCF#1 retrieves the destination information for the new session, and invokes whatever service logic is appropriate for this new session.

12. S-CSCF#1 determines the network operator addressed by the destination URL, and forwards the INVITE to S-CSCF#2 (or I-CSCF#2, the public entry point for S-CSCF#2).

13. S-CSCF#2 decodes the private URL destination, and determines the final destination of the new session. It determines the network operator addressed by the destination URL. The request is then forwarded onward to S-CSCF#F as in a normal session establishment

14. S-CSCF#F invokes whatever service logic is appropriate for this new session, and forwards the request to P-CSCF#F

15. P-CSCF#F forwards the request to UE#F

16-21. The normal session establishment continues through bearer establishment, optional alerting, and reaches the point when the new session is accepted by UE#F. UE#F then sends the 200-OK final response to P-CSCF#F, which is forwarded through S-CSCF#F, S-CSCF#2, S-CSCF#1, P-CSCF#1, to UE#1. At this point a new session is successfully established between UE#1 and UE#F.

22-26. The Refer request was successful, and UE#1 sends a 200-OK final response to UE#2. This response is sent through P-CSCF#1, S-CSCF#1, S-CSCF#2, P-CSCF#2, and to UE#2.

27-31. UE#1 clears the original session with UE#2 by sending the BYE message. This message is routed through P-CSCF#1, S-CSCF#1, S-CSCF#2, P-CSCF#2, to UE#2.

32-36. UE#2 acknowledges the BYE and terminates the original session. It responds with the 200-OK response, routed through P-CSCF#2, S-CSCF#2, S-CSCF#1, P-CSCF#1, to UE#1.

5.11.6.2 Application to Session Transfer Services

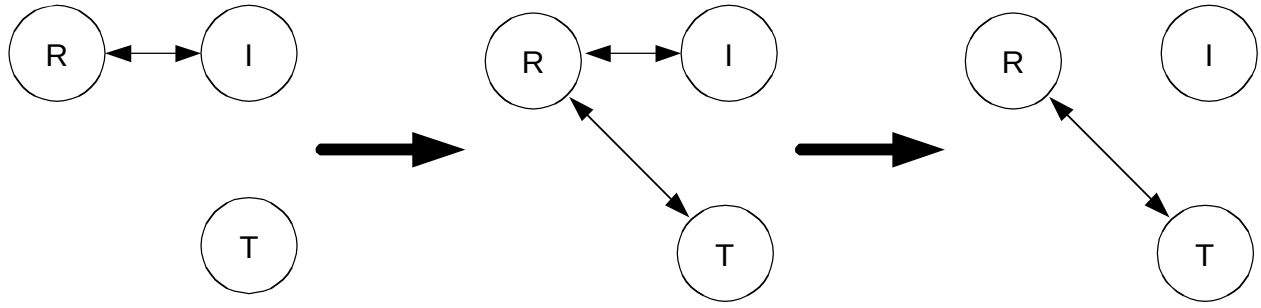
5.11.6.2.0 General

This section shows how the Refer primitive given above can be used to provide common session-transfer services.

5.11.6.2.1 Blind Transfer and Assured Transfer

A Blind Transfer starts with an existing session, established between the Initiator (I) and the Recipient (R). In a typical case, this session was actually initiated by R. In the end it is desired that the Recipient has a session with the Target (T).

From the starting configuration, shown in the leftmost diagram, I sends a Refer message to R, who then initiates a session with the Target (T), as shown in the middle diagram. Immediately after sending the Refer message to R, I issues the BYE message to terminate its connection with R. The end configuration is shown in the rightmost diagram.



An Assured Transfer is identical to the above, except that I waits until the Refer successfully completes before issuing the BYE message to terminate its connection with R. If the new session from R to T were to fail, R would still have a session with I.

**** Next Change ****

5.12 Mobile Terminating call procedures to unregistered Public User Identities

5.12.0 General

This section describes information flows for the procedures of Mobile Terminating call flows for unregistered IMS Public User Identities. The detection of an unregistered Public User Identity is done in HSS and if this Public User Identity has services related to unregistered state, a S-CSCF is selected for the unregistered Public User Identity. S-CSCF performs whatever further actions are appropriate for the call attempt to the unregistered IMS Public User Identity.

Two basic examples for "services related to unregistered" are call redirection to CS domain and voice mailbox service. Call redirection to CS domain is supported to cover the cases when the UE is not registered in IMS but can be reached via the CS domain. Then, a temporary S-CSCF is selected and performs whatever further actions are appropriate for the call attempt.

The principle established in sub-clause 4.3.3.4, where the public user identifiers for the same profile are allocated to the same S-CSCF, is followed.

5.12.1 Mobile Terminating call procedures to unregistered Public User Identity that has services related to unregistered state

In Figure 5.43 below the Public User Identity is unregistered for IMS and the Public User Identity has services related to unregistered state. In this case, the HSS responds back to I-CSCF with an indication that I-CSCF should select S-CSCF for this MT call to the unregistered Public User Identity of the user or provide the I-CSCF with the previously allocated S-CSCF name. Before S-CSCF selection, I-CSCF shall query HSS for the information related to the required S-CSCF capabilities. I-CSCF selects a S-CSCF to invoke service logic and I-CSCF routes the call further to the selected destination. If the S-CSCF does not have the relevant information from the user profile then the S-CSCF shall download the relevant information from HSS before it invokes service logic and any further actions in the call attempt. The service implemented by this information flow could be e.g. “Call Forward Unconditional.”

This is shown by the information flow in Figure 5.43:

**** Next Change ****

5.13 IMS Emergency Sessions

5.13.0 General

This section presents the main procedures for the IMS emergency sessions.

5.13.1 Requirements for IMS Emergency Sessions

A CS capable UE shall use the CS domain for emergency services. In addition, the solution for emergency sessions in the IMS shall fullfil the following capability requirements:

1. It should be independent from the used underlying IP connectivity network with respect to the detection and routing of emergency sessions.
2. Any kind of emergency numbers, all kinds of emergency SIP URIs and special indications for emergency sessions within the SIP signalling must be supported (especially IETF proposals on adressing should be taken into consideration).
3. Emergency sessions should be prioritized over “ordinary” sessions by the system.
4. Setup of IMS emergency sessions shall be possible for users with a barred public user identity.
5. The primary solution shall be that the UE can detect an emergency session (e.g. by evaluating the SIP-URI or the dialed number) by itself and indicates the emergency session to the network. But the specification must also support cases where the UE can’t detect an emergency session.
6. The solution must work in case the UE has a UICC card and is registered to the IMS or not, as well as in the UICC-less case. In the UICC-less and non-registered cases it must be possible to setup a bearer in the IP connectivity network and session setup must be possible without an existing security association between UE and P-CSCF.
7. Emergency Service is not a subscription service and therefore will normally be supported entirely in the serving network and provided without interaction with a “Home” network in a roaming case.
8. The solution shall also work in a roaming case when the session establishment is routed via a P-CSCF located in the home network. In this case the home network should be able to detect that the session is for emergency service (whether indicated as such or not) and route emergency sessions to an emergency center in the roaming country (i.e. where the user is geographically located).
9. Alternatively, the home network may respond to the UE indicating that the UE should initiate an emergency session in the serving network (e.g. via the CS domain of the serving network). The solution should be in principle similar for both scenarios (considering e.g. the entities, which perform session control and detection of emergency situations).
10. Emergency centers may be connected to the CS domain, PS domain or any other packet network.
11. Emergency centres shall be able to call back the user.

The solution for emergency sessions shall also fulfil the following architectural requirements:

1. The architecture for Emergency Service should be driven by the specific capabilities requirements. To the extent that existing IMS functional entities can be re-used, this should be done. However the specification should not be constrained by the existing functional entities.
2. The architecture should take into account that it may be possible to make emergency calls on other media than voice. It needs to take account support, for example, the deaf and hearing-impaired using a text phone that might generate information, for example, using IMS messaging procedures. There may also be a need to work with phones that attempt the emergency call as a videotelephony call.

5.13.2 Procedures for SIP Emergency Session Establishment

It shall be possible for the network to discriminate between emergency sessions and other sessions. This shall allow special treatment (e.g. with respect to filtering, higher priority, routing, QoS) of emergency sessions.

The P-CSCF in the visited or home network is the IMS network entity, which always detects an emergency session. The P-CSCF should route the corresponding request to an S-CSCF, which is able to handle emergency sessions. P-CSCF and S-CSCF shall be located in the same network. Alternatively, the home network may respond to the UE indicating that the UE should initiate an emergency session in the serving network (e.g. via the CS domain of the serving network). Based on location information provided by the UE and the location of the S-CSCF, the S-CSCF shall route the emergency request directly to an emergency centre, to an I-CSCF or BGCF.

5.13.3 Procedures for IMS Emergency Session Establishment

In order to establish an IMS emergency session the UE needs to have IP-CAN bearers to be used for IMS related signalling and for the media related to the emergency session.

5.14 Interactions involving the MRFC/MRFP

5.14.0 General

The MRFC/MRFP are resources of the IMS that provide support for bearer related services such as for example multi-party sessions, announcements to a user or bearer transcoding. This section describes how the resources of the MRFC/MRFP are used.

5.14.1 Interactions between the UE and the MRFC

In some cases an operator may wish to make an MRFC available directly to a UE, for example to support ad-hoc multi-party sessions to be initiated by the UE. In this case, the operator advertises the name of one or more MRFCs and a UE will invite an MRFC to a session. The session invitation would need to contain additional information indicating the specific capabilities (e.g., multi-party) desired. A conference ID would be assigned by the MRFC and returned to the UE. This would then be used by the UE in subsequent interactions with the MRFC and other UEs participating in the session.

There are two approaches to invite new participants to the multiparty session. In the first, a UE directs other UEs to join the multiparty session based on the use of the SIP REFER method. This allows session invitations with consultation. In the second method, the MRFC uses information received from a UE e.g. within a list of session participants to invite other UEs to the multiparty session. This allows session invitations without consultation.

5.14.2 Service control based interactions between the MRFC and the AS

The MRFC/MRFP resources may also be used, based on service control in an IMS network, for services such as multiparty sessions, announcements or transcoding. In this case an Application Server interacts with an MRFC. Session control messages are passed between the AS and the MRFC via the S-CSCF.

There are two approaches for the AS to control the sessions. In the first, the AS uses 3rd party call control. The second approach uses the SIP REFER method.

In either case, the appropriate service in the AS would be triggered by a UE initiated SIP message containing information indicating the specific capabilities desired. This session invitation would also carry additional information indicating the specific capabilities (e.g., multi-party). A conference ID would be assigned by the MRFC and would be used by the AS in subsequent interactions with the MRFC in INVITE messages connecting other endpoints.

3rd party call control can also be used to invite announcement and transcoding services. That is, the AS will send an INVITE to the MRFC with an indication of the capability being requested and with additional information related to the specific service such as identification of the announcement to be played or identification of the specific transcoding requirements.

5.14.3 Interactions for services using both the Ut interface and MRFC capabilities

Network services hosted on an AS and configurable by the user via the Ut interface may also use the capabilities provided by the MRFC. For this case, the AS either supports MRFC capabilities, or communicates with an MRFC.

Communications across the Ut interface between the UE and the AS allow the UE to securely manage and configure data for such services (e.g. conference type services). Means for the AS to propagate this management and configuration information to the MRFC is not standardized in this Release.

5.15 Mobile Terminating session procedure for unknown user

5.15.0 General

This section describes information flows Mobile Terminating procedure for an unknown user. The unknown user cases include those where session requests are made towards public user identities that are incorrect, un-issued or have been cancelled/deleted. The determination of unknown user is carried out in the HSS and/or the SLF (for networks that require SLF functionality). The information flows of figures 5.45 and 5.46 illustrate how SIP messages can be used to inform the requesting party that the requested user is not known within the network.

5.15.1 Unknown user determined in the HSS.

In Figure 5.45 the unknown status of the requested party is determined in the HSS. The I-CSCF requests information on the user to be reached and the HSS responds back to the I-CSCF with an indication that the user is unknown. The I-CSCF uses the indication that the user is unknown returned from the HSS to formulate the correct SIP message back towards the originating party to inform them that the user is unknown. The case where the SLF determines unknown status is in section 5.15.2. The flows of figure 5.45 could include SLF determination of the HSS, however these are not shown for clarity.

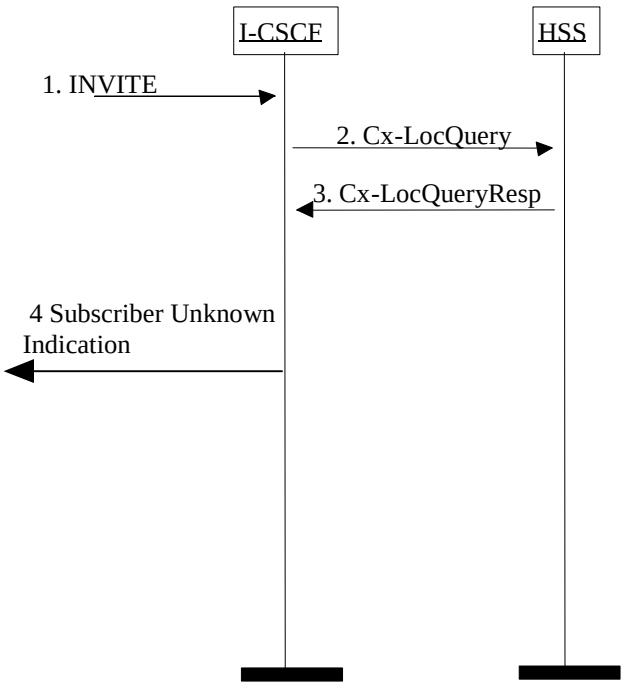


Figure 5.45 HSS determination of unknown user.

1) I-CSCF receives an INVITE.
2) I-CSCF queries the HSS for current location information.
3) HSS responds with an indication that the user is unknown
4) The I-CSCF responds to the origin of the request that the user is unknown.

5.15.2 Unknown user determined in the SLF

In Figure 5.46 the unknown status of the requested party is determined in the SLF. The I-CSCF requests information on the user to be reached and the SLF responds back to the I-CSCF with an indication that the user is unknown. The I-

CSCF uses the indication that the user is unknown returned from the SLF to formulate the correct SIP message back towards the originating party to inform them that the user is unknown.

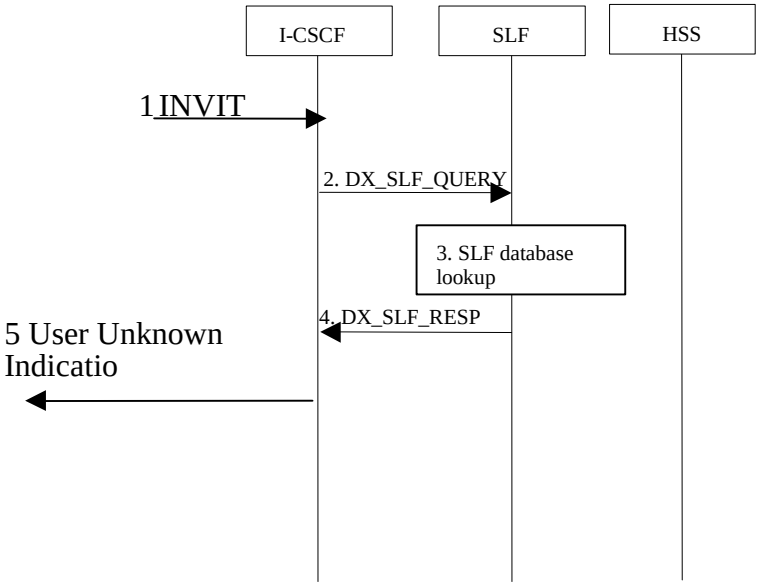


Figure 5.46 SLF determination of unknown user.

1) The ICSCF receives an INVITE request and now has to query for the location of the user's subscription data.
2) The I-CSCF sends a DX_SLF_QUERY to the SLF and includes as parameter the user identity which is stated in the INVITE request.
3) The SLF looks up its database for the queried user identity.
4) The SLF answers with an indication that the user is unknown.
5) The I-CSCF responds to the origin of the request that the user is unknown.

5.16 IMS messaging concepts and procedures

5.16.0 General

This clause describes architectural concepts and procedures for providing Messaging in the IM CN Subsystem. The service enablers for Messaging and possible reuse of IMS service enablers within this context as well security and charging expectations, addressing, privacy, content handling and limitations, filtering, media types and message lengths, etc. are to be further studied.

Any ISIM related architectural requirements would be studied as part of overall IMS Messaging.

5.16.1 Immediate Messaging

5.16.1.0 General

This sub-clause describes architectural concepts and procedures for fulfiling the requirements for Immediate Messaging described in TS 22.340 [29a].

5.16.1.1 Procedures to enable Immediate Messaging

5.16.1.1.0 General

IMS users shall be able to exchange immediate messages with each other by using the procedure described in this sub-clause. This procedure shall allow the exchange of any type of multimedia content (subject to possible restrictions based on operator policy and user preferences/intent), for example but not limited to:

- Pictures, video clips, sound clips with a format defined by 3GPP TS 26.xxx [37]

The sender UE can include an indication in the message regarding the length of time the message will be considered valid.

5.16.1.1.1 Immediate messaging procedure to registered public user identity

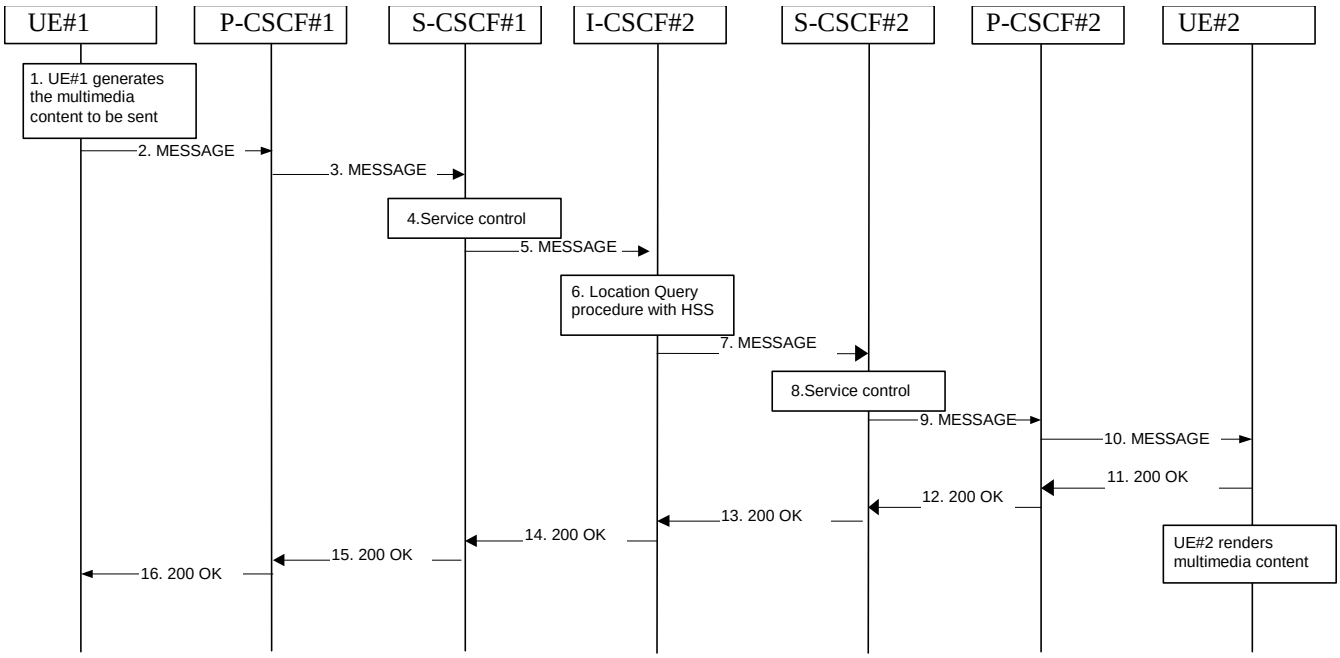


Figure 5.47: Immediate Messaging procedure to registered public user identity

1. UE#1 generates the multimedia content intended to be sent to UE#2.
2. UE#1 sends the MESSAGE request to P-CSCF#1 that includes the multimedia content in the message body.
3. P-CSCF#1 forwards the MESSAGE request to S-CSCF#1 along the path determined upon UE#1's most recent registration procedure.
4. Based on operator policy S-CSCF#1 may reject the MESSAGE request with an appropriate response, e.g. if content length or content type of the MESSAGE are not acceptable. S-CSCF#1 invokes whatever service control logic is appropriate for this MESSAGE request. This may include routing the MESSAGE request to an application server, which processes the request further on.
5. S-CSC#1 forwards the MESSAGE request to I-CSCF#2.
6. I-CSCF#2 performs Location Query procedure with the HSS to acquire the S-CSCF address of the destination user (S-CSCF#2).
7. I-CSCF#2 forwards the MESSAGE request to S-CSCF#2.
8. Based on operator policy S-CSCF#2 may reject the MESSAGE request with an appropriate response, e.g. if content length or content type of the MESSAGE are not acceptable. S-CSCF#2 invokes whatever service control logic is appropriate for this MESSAGE request. This may include routing the MESSAGE request to an application server, which processes the request further on.

For example, the UE#2 may have a service activated that blocks the delivery of incoming messages that fullfill criterias set by the user. The AS may then respond to the MESSAGE request with an appropriate error response.

9. S-CSCF#2 forwards the MESSAGE request to P-CSCF#2 along the path determined upon UE#2's most recent registration procedure.

10. P-CSCF#2 forwards the MESSAGE request to UE#2. After receiving the MESSAGE UE#2 renders the multimedia content to the user.

11. – 16. UE#2 acknowledges the MESSAGE request with a response that indicates that the destination entity has received the MESSAGE request. The response traverses the transaction path back to UE#1.

**** Next Change ****

5.16.2 Session-based Messaging

5.16.2.0 General

This subclause describes architectural concepts and procedures for fulfiling the requirements for Session-based Messaging described in TS 22.340 [29a].

5.16.2.1 Architectural principles

Session-based IMS messaging communications shall as much as possible use the same basic IMS session delivery mechanisms (e.g. routing, security, service control) as defined in clause 4 and 5 of this document. For session based messaging the session shall include a messaging media component, other media components may also be included. Once the session containing a messaging media component is established, messages in the session are transported between the session participants as per the parameters defined in the messaging media component part of the session description (SDP).

For addressing chat-group-type session based messaging the concept of Public Service Identities is used.

Session based messaging is available for users that are registered in the IMS.

The session based messaging shall be able to provide the following functionality:

-Per-message-based charging, as well as content- and size-based charging.

-Operator-controlled policy to be set on the size and content of the messages.

-Support for a messaging media component as part of a session where other media components are also included.

-Support for messaging-only sessions.

5.16.2.2 Procedures to enable Session based Messaging

5.16.2.2.0 General

IMS users shall be able to exchange session-based messages with each other by using the procedure described in this sub-clause. This procedure shall allow the exchange of any type of multimedia content (subject to possible restrictions based on operator policy and user preferences/intent), for example but not limited to:

- Pictures, video clips, sound clips with a format defined by 3GPP TS 26.xxx [37]

5.16.2.2.1 Session based messaging procedure to registered public user identity

Editor's note: This sub-clause will describe session based messaging between two UEs.

5.16.2.2.2 Session based messaging procedure using multiple UEs

Editor's note: This sub-clause will describe session based messaging between multiple UEs using for example a Chat session.

5.17 Refreshing sessions

The active sessions in stateful network elements (e.g. CSCFs, ASs) may need to be refreshed periodically. This allows these stateful elements to detect and free resources that are being used by hanging sessions.

This SIP-level session refreshing mechanism is to be used to allow removing session state from the stateful elements of the session path upon unexpected error situations (e.g. loss of radio coverage, crash of application in the UE, etc…). The refreshing period is typically in the range of several tens of minutes / hours. The mechanism is intended as a complementary mechanism for the "Network initiated session release" described in sub-clause 5.10.3. Whether the session refresh mechanism is used for a particular session is negotiated between the endpoints of the session upon session initiation.

IMS entities acting as User Agents as defined in RFC 3261 [12] should support the refresh mechanism of SIP sessions. This includes support for the negotiation of the session refresh details upon session initiation, and the initiation of session refresh requests.

5.18 Architecture scenarios for IP version Interworking

5.18.0 General

The IP version interworking should not adversely affect IMS sessions that are primarily IPv6 only.
The network shall, at a minimum, support mechanisms that support IP version interworking for UEs, which comply with previous release of specifications. In addition, any impacts due to specific properties of the IP CAN shall be taken care of by the IP-CAN itself without affecting the IMS. One possible architecture scenario can be based on the principle defined in 3GPP TS 23.221[7] using gateways.

Figure 5.49 shows a high-level architecture diagram for one interworking model. In this case, the TrGW is a NA(P)T-PT providing the translation function.

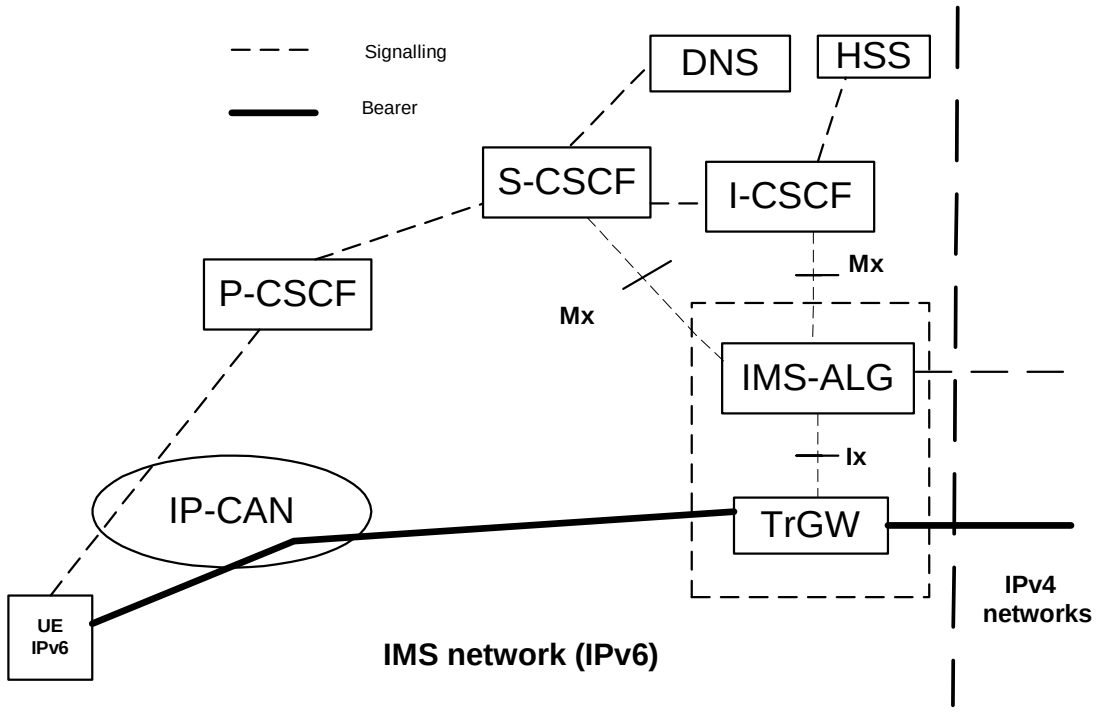


Figure 5.49 General IP version interworking principle with TrGW

It is FFS whether there are any additional mechanisms (other than the principles described here) that can be used for IMS IP version interworking.

Note that the standardisation and functional requirements of Ix reference point are FFS.

The Mx reference point allows S-CSCF/I-CSCF to communicate with an IMS ALG function in order to provide interworking with IPv4 SIP networks. It is FFS whether both S-CSCF and I-CSCF need to communicate with the IMS ALG.

Note that the procedure of inserting the IMS ALG (e.g. which CSCF is responsible) in relation to originating and terminating sessions are for FFS.

5.18.1 Originating Session Flows towards IPv4 SIP network

Note this section will contain high-level session flow and interaction for originating session.

**** Next Change ****

Annex E (normative): IP-Connectivity Access Network specific concepts when using GPRS to access IMS

E.0 General

This clause describes the main IP-Connectivity Access Network specific concepts that are used for the provisioning of IMS services over GPRS access with a GERAN and/or UTRAN radio access.

When using GPRS-access, the IP-Connectivity Access Network bearers are provided by PDP Context(s).

E.1 Mobility related concepts

E.1.0 General

The Mobility related procedures for GPRS are described in TS 23.060 [23] and the IP address management principles are described in TS 23.221 [7]. As specified by the GPRS procedures, the UE shall acquire the necessary IP address(es) as part of the PDP context activation procedure(s).

If an UE acquires a new IP address due to changes triggered by the GPRS/UMTS procedures or by changing the IP address according to [7], the UE shall re- register in the IMS by executing the IMS registration;

When the PLMN changes, and the attempt to perform an inter-PLMN routeing area update is unsuccessful, then the UE should attempt to re-attach to the network using GPRS procedures and re-register for IMS services. Typically this will involve a different GGSN.

E.1.1 Procedures for P-CSCF discovery

E.1.1.0 General

This clause describes the P-CSCF discovery procedures applicable for GPRS access. These procedures follow the generic mechanisms described in clause 5.1.1, hence the following applies:

P-CSCF discovery shall take place after GPRS attach and after or as part of a successful activation of a PDP context for IMS signalling using one of the following mechanisms:

1. Transfer a Proxy-CSCF address within the PDP Context Activation signalling to the UE, as described in sub-clause E.1.1.1. The UE shall request the P-CSCF address(es) from the GGSN when activating the PDP context. The GGSN shall send the P-CSCF address(es) to the UE when accepting the PDP context activation. Both the P-CSCF address(es) request and the P-CSCF address(es) shall be sent transparently through the SGSN.

2. Use of DHCP to provide the UE with the domain name of a Proxy-CSCF and the address of a Domain Name Server (DNS) that is capable of resolving the Proxy-CSCF name, as described in clause 5.1.1.

When using DHCP/DNS procedure for P-CSCF discovery (according to the mechanisms described in sub-clause 5.1.1.1) with GPRS-access, the GGSN acts as DHCP Relay agent relaying DHCP messages between UE and the DHCP server.

E.1.1.1 GPRS procedure for P-CSCF discovery

This alternative shall be used for UE(s) not supporting DHCP. This may also be used for UE(s) supporting DHCP.

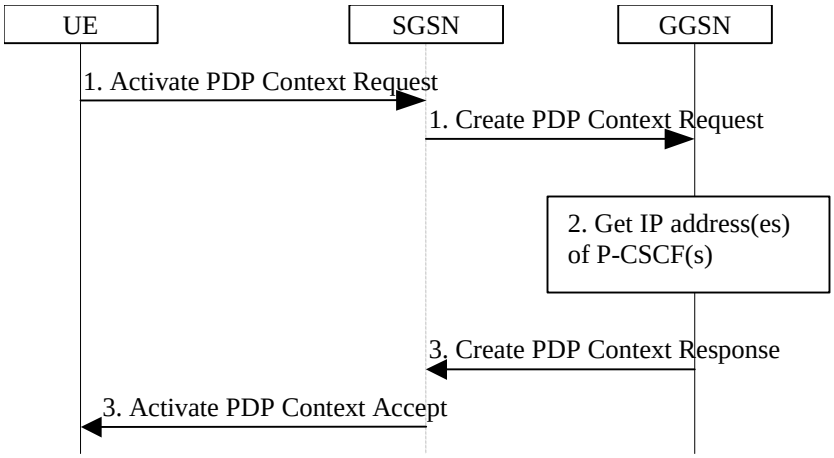


Figure E.1: P-CSCF discovery using PDP Context Activation signalling

1. The UE requests establishment of a PDP context according to section 4.2.6 (QoS requirements for IM CN subsystem signalling). The UE indicates that it requests a P-CSCF IP address(es). The indication is forwarded transparently by the SGSN to the GGSN.

2. The GGSN gets the IP address(es) of the P-CSCF(s). The mechanism to do this is a matter of internal configuration and is an implementation choice.

3. If requested by the UE, the GGSN includes the IP address(es) of the P-CSCF(s) in the Create PDP Context Response. The P-CSCF address(es) is forwarded transparently by the SGSN to the UE.

After reception of the IP address of a P-CSCF the UE may initiate communication towards the IM subsystem.

Note: This request of a P-CSCF IP address(es) and response is not transparent for pre-R5 SGSN when using the Secondary PDP Context Activation Procedure as defined in TS 23.060 [23].

E.2 QoS related concepts

E.2.1 Application Level Signalling for IMS

E.2.1.0 General

When the UE uses GPRS-access for IMS services, it shall be able to establish a dedicated signalling PDP-Context for IM Subsystem related signalling or utilize a general-purpose PDP context for IM subsystem signalling traffic.

E.2.1.1 QoS Requirements for Application Level Signalling

The UE shall be able to request prioritised handling over the radio for IM Subsystem related signalling by including the Signalling Indication in the QoS IE of the PDP Context to be used for this traffic as described in TS 23.207.

**** Next Change ****

E.2.2 The QoS requirements for an IM CN subsystem session

E.2.2.0 General

The selection, deployment, initiation and termination of QoS signalling and resource allocation shall consider

- the general requirements described in clause 4.2.5.
- and the requirements described in this clause so as to guarantee the QoS requirement associated with an IM CN subsystem session when using GPRS access for IMS services.

1. QoS Signalling at Different Bearer Service Control Levels

   During the session set-up in a IM CN subsystem, at least two levels of QoS signalling/negotiation and resource allocation should be included in selecting and setting up an appropriate bearer for the session:

   a. The QoS signalling/negotiation and resource allocation at the IP Bearer Service (BS) Level:

      The QoS signalling and control at IP BS level is to pass and map the QoS requirements at the IP Multimedia application level to the UMTS BS level and performs any required end-to-end QoS signalling by inter-working with the external network. The IP BS Manager at the UE and the GGSN is the functional entity to process the QoS signalling at the IP BS level.

   b. The QoS signalling/negotiation and resource allocation at the UMTS Bearer Service Level:

      The QoS signalling at the UMTS BS Level is to deliver the QoS requirements from the UE to the RAN, the CN, and the IP BS manager, where appropriate QoS negotiation and resource allocation are activated accordingly. When UMTS QoS negotiation mechanisms are used to negotiate end-to-end QoS, the translation function in the GGSN shall co-ordinate resource allocation between UMTS BS Manager and the IP BS Manager.

   Interactions (QoS class selection, mapping, translation as well as reporting of resource allocation) between the QoS signalling/control at the IP BS Level and the UMTS BS Level take place at the UE and the GGSN which also serve as the interaction points between the IM CN subsystem session control and the UMTS Bearer QoS control.

   UMTS specific QoS signalling, negotiation and resource allocation mechanisms (e.g. RAB QoS negotiation and PDP Context set-up) shall be used at the UMTS BS Level. Other QoS signalling mechanisms such as RSVP at the IP BS Level shall only be used at the IP BS Level.

It shall be possible to negotiate a single resource allocation at the UMTS Bearer Service Level and utilise it for multiple sessions at the IP Bearer Service Level.

E.2.2.1 Relation of IMS media components and PDP contexts carrying IMS media

The relation between IMS media components and PDP contexts carrying IMS media is controlled by the IMS network on media component level in the following way:

The P-CSCF shall have the capability to indicate to the UE that a separate PDP Context is required for each IMS media component indicated.The P-CSCF shall apply and maintain the same policy to separate specific media components into separate PDP Contexts during a session. If a media component is added during the session, the new decision on the separation for the media components shall not contradict any former decisions. For mobile originating sessions the P-CSCF shall apply the policy to the initial offer to ensure identical decisions for different answers, e.g. a media component not required to use a separate PDP Context initially, shall not later require a separate PDP Context (e.g. in case of subsequent answers received due to forking).

- If the UE receives such an indication for a media component, it shall open a separate PDP Context for this media component. If the UE receives no such indication for a media component, the UE makes the decision whether to open a separate PDP Context or modify an existing PDP Context for this media component.

- The criteria and information for setting this indication is determined by local policy in the network where the P-CSCF is located.

Note: the bearer charging capabilities of the P-CSCF's network, and the capabilities of deployed UEs should be taken into account when defining such policies in the visited IMS network operator's domain.

- The IMS network shall have the capability to transfer the media component level indication described above to the UE. This media component level indication shall be transferred in SIP/SDP signaling upon session initiation and addition of media component(s) to active IMS sessions.

It is assumed that media components from different IMS sessions are not carried within the same PDP context.

All associated IP flows (such as e.g. RTP / RTCP flows) used by the UE to support a single media component are assumed to be carried within the same PDP context.

E.2.3 Interaction between GPRS QoS and session signaling

E.2.3.0 General

The generic mechanisms for interaction between QoS and session signaling are described in clause 5.4.7, the mechanisms described there are applicable to GPRS-access as well.
This clause describes the GPRS-access-specific concepts.

At PDP context setup the user shall have access to either GPRS without service-based local policy, or GPRS with service-based local policy. The GGSN shall determine the need for service-based local policy, possibly based on provisioning and/or based on the APN of the PDP context.

For the GPRS without service-based local policy case, the bearer is established according to the user’s subscription, local operator’s IP bearer resource based policy, local operator's admission control function and GPRS roaming agreements. The establishment of the PDP context bearer shall use the PDP context activation procedure specified in TS 23.060.

For the GPRS with service-based local policy case, Service-Based Local Policy decisions (e.g., authorisation and control) are also applied to the bearer.

The GGSN contains a Policy Enforcement Function (PEF).

E.2.3.1 Resource Reservation with Service-based Local Policy

The request for GPRS QoS resources may be signaled independently from the request for IP QoS resources by the UE. At the GPRS BS Level, the PDP Context activation shall be used for QoS signaling. At the IP BS Level, RSVP may be used for QoS signaling.

E.2.4 Network initiated session release - P-CSCF initiated

E.2.4.0 General

In the event of loss of coverage, 3GPP TS 23.060 defines the Iu or RAB Release procedures. In case of PDP context with streaming or conversational class the maximum bitrate of the GTP tunnel between SGSN and GGSN is modified to 0 kbit/s in up- and downlink direction. This is indicated to the P-CSCF / PDF by performing the 'Indication of PDP Context Modification' procedure (see 3GPP TS 23.207) as shown in Figure E.2. For loss of coverage in case of other PDP contexts (background or interactive traffic class), the PDP context is preserved with no modifications and therefore no indication to the P-CSCF/PDF.

E.2.4.1 Network initiated session release - P-CSCF initiated after loss of radio coverage

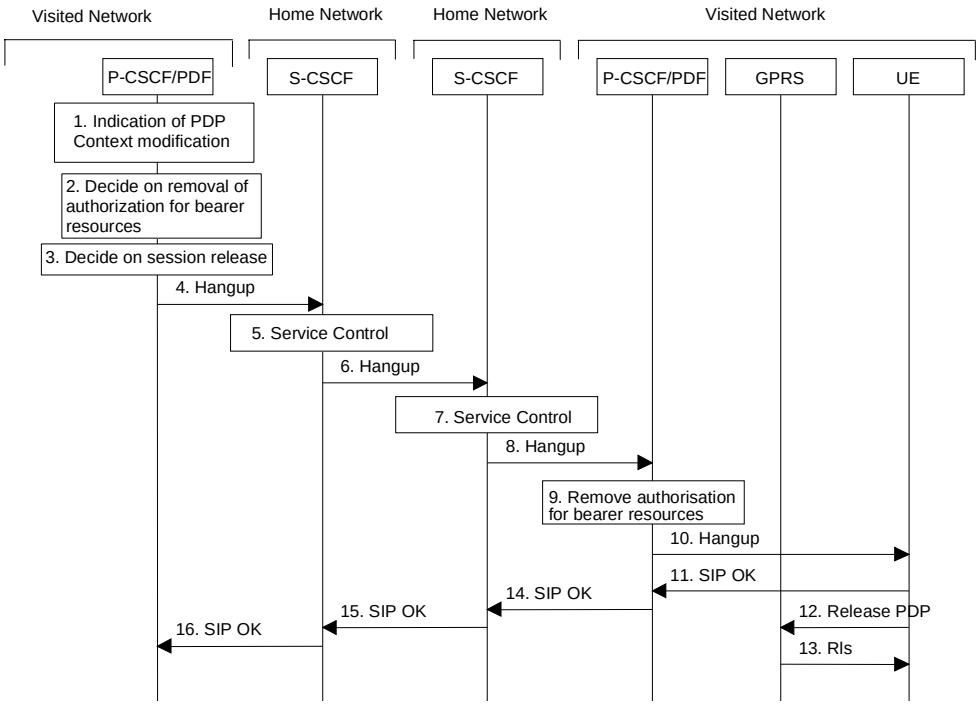


Figure E.2: Network initiated session release - P-CSCF initiated after loss of radio coverage

1. In the event of loss of radio coverage for a PDP context with streaming or conversational class the maximum bitrate of the GTP tunnel between SGSN and GGSN is modified to 0 kbit/s in up- and downlink direction. The P-CSCF/PDF receives an indication of PDP context modification.

2. It is optional for the P-CSCF/PDF to deactivate the affected bearer and additional IP bearers (e.g. an IP bearer for chat could still be allowed). For these IP bearers the P-CSCF/PDF performs the 'Revoke Authorization for UMTS and IP Resources' procedure (see 3GPP TS 23.207). If the P-CSCF decides to terminate the session then the P-CSCF/PDF removes the authorisation for resources that had previously been issued for this endpoint for this session.

3. The P-CSCF decides on the termination of the session. If the P-CSCF decides to terminate the session then the P-CSCF/PDF removes the authorisation for resources that had previously been issued for this endpoint for this

session. The P-CSCF/PDF shall perform the 'Revoke Authorization for UMTS and IP Resources' procedure (see 3GPP TS 23.207) in case that all IP bearers associated with the session have not been deleted yet.

The following steps are only performed in case the P-CSCF/PDF has decided to terminate the session.

4. The P-CSCF generates a Hangup (Bye message in SIP) to the S-CSCF of the releasing party.
5. The S-CSCF invokes whatever service logic procedures are appropriate for this ending session.
6. The S-CSCF of the releasing party forwards the Hangup to the S-CSCF of the other party.
7. The S-CSCF invokes whatever service logic procedures are appropriate for this ending session.
8. The S-CSCF of the other party forwards the Hangup on to the P-CSCF.
9. The P-CSCF/PDF removes the authorisation for resources that had previously been issued for this endpoint for this session. This step also results in a release indication to the GPRS subsystem to confirm that the IP bearers associated with the session have been deleted for UE#2.
10. The P-CSCF forwards the Hangup on to the UE.
11. The UE responds with an acknowledgement, the SIP OK message (number 200), which is sent back to the P-CSCF.
12. Steps 12 and 13 may be done in parallel with step 11. The UE initiates the release of the bearer PDP context.
13. The GPRS subsystem releases the PDP context. The IP network resources that had been reserved for the message receive path to the UE for this session are now released. This is initiated from the GGSN. If RSVP was used to allocated resources, then the appropriate release messages for that protocol would invoked here.
14. The SIP OK message is sent to the S-CSCF.
15. The S-CSCF of the other party forwards the OK to the S-CSCF of the releasing party.
16. The S-CSCF of the releasing party forwards the OK to the P-CSCF of the releasing party.

3GPP TSG-SA2 Meeting #37
Innsbruck, Austria, 12 – 16 January 2004

Tdoc S2-040440

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **394** ⌘ **rev** **2** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	PSI clean-up
Source:	⌘	SA2 (Nokia)
Work item code:	⌘	IMS2
Date:	⌘	15/01/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The concept of Public Service Identities has been developped, mechanisms for routing to and from PSIs have been incorporated into the TS. However, the description of some of the concepts invloved is incomplete and not fully accurate.
Summary of change:	⌘	The means for configuring PSIs in the HSS is clarified. Some other aspects around routing are also clarified.
Consequences if not approved:	⌘	Inaccurate description would make stage-3 design difficult.

Clauses affected:	⌘	5.4.12.1, 5.4.12.2, 5.4.12.3, 5.4.12.4			
Other specs affected:	⌘	**Y**	**N**		
			X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

5.4.12 Configuration and Routing principles for Public Service Identities

Depending on the service nature, different mechanisms may be used for configuration and routing of PSIs according to operator preference.

When PSIs are created, the uniqueness of a PSI shall be ensured. Note that only the username part of a PSI is definable within a predefined hostname(s).

Whenever possible, routing to/from a Public Service Identity (PSI) should be provided using basic principles used for IMS routing.

5.4.12.1 PSIs on the originating side

The application server hosting the PSI may be invoked as an originating application server. This can be achieved by modifying the filter information within the subscription information of the users intending to use the service identified by the PSI. The PSI is then made available to these users.

The SIP requests are directed to the corresponding application server hosting the service according to the originating filtering rules in the S-CSCF of the user who is using the service.

Such statically pre-configured PSIs are only ~~available~~ accessible internally from within the IMS of the operator's domain where the PSI is configured.

5.4.12.2 PSIs on the terminating side

The application server hosting the PSI may be invoked as a terminating application server via information stored in the HSS. ~~with the AS and related PSIs configured in the home network, e.g. HSS.~~ Such PSIs are globally routable and can be made available to users within and outside the operator domain, and can take the following form:

- Distinct PSIs (e.g. sip:my_service@example.com). Distinct PSIs can be created, modified and deleted in the HSS by the operator via O&M mechanisms. Distinct PSIs can also be created and deleted by users using the Ut interface using the means described in sub-clause 5.4.12.3 for subdomain-based PSIs. The distinct PSI may then be created in the HSS by the AS using the Sh interface.

- Wildcarded PSIs (sip:chatlist_*@example.com): A range of PSIs with the same domain part in the SIP URI is defined using a wildcard indication in the userpart of the SIP-URI. Wildcarded PSI ranges can be created, modified and deleted in the HSS by the operator via O&M mechanisms. Specific PSIs within a wildcarded range can be created and deleted by users using the Ut interface to the AS hosting the wildcarded range, or by the operator via O&M mechanisms.

~~Distinct PSIs can be created or deleted, by the users using the Ut interface, or by the operator via O&M mechanisms.~~

For both the distinct PSIs and wildcarded PSIs, there are two ways to route towards the AS hosting the PSI:

a) The HSS maintains the assigned S-CSCF information and ISC Filter Criteria information for the "PSI user" to route to the AS hosting the PSI according to IMS routing principles. In this case, the I-CSCF receives SIP requests at the terminating side, queries the HSS and directs the request to the S-CSCF assigned to the "PSI user". The S-CSCF forwards the session to the application server hosting the PSI according to the terminating ISC Filter Criteria.

b) The HSS maintains the address information of the AS hosting the PSI for the "PSI user". In this case, the AS address information for the PSI is returned to the I-CSCF in the location query response, in which case the I-CSCF will forward the request directly to the AS hosting the PSI.

~~In this case, t~~The AS hosting the PSI in combination with its entry in the HSS is referred to as "PSI user".

Figure 5.4.12.a depicts a routing example for incoming session where the session request is routed directly to the AS hosting the PSI.

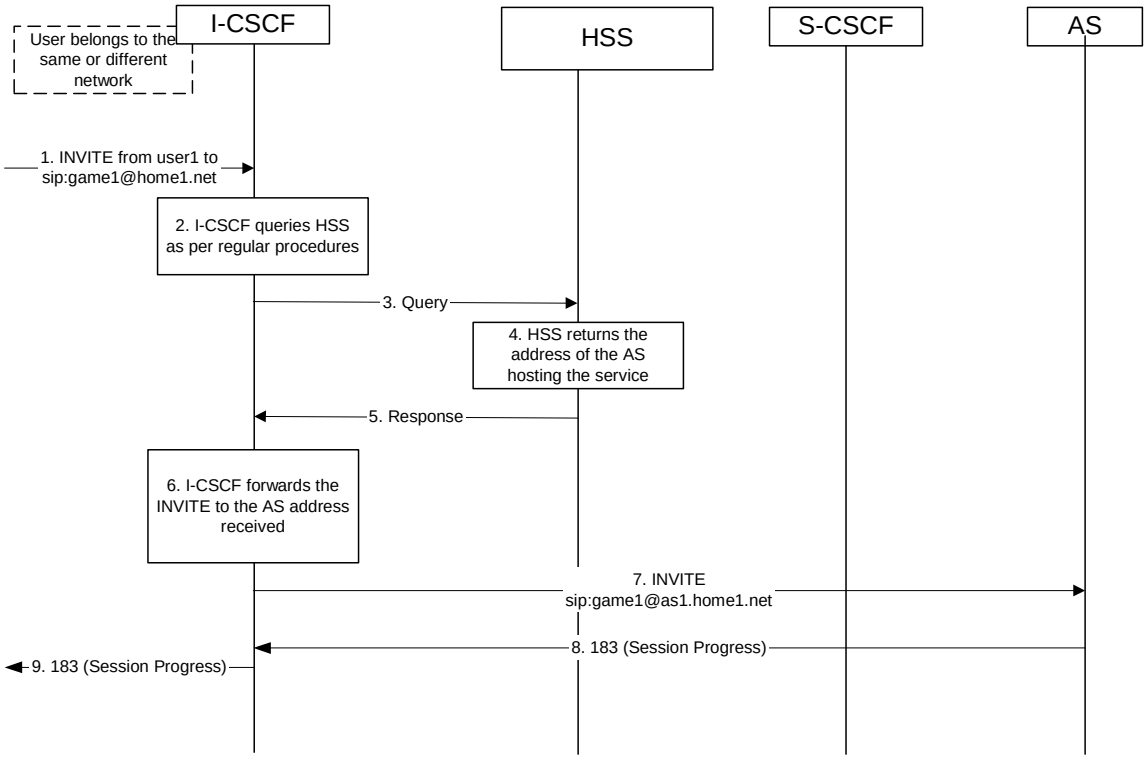


Figure 5.4.12.a Incoming session, direct route towards the AS

1. I-CSCF receives a request destined to the PSI.

2-3. I-CSCF queries the HSS in order to determine the next hop in the routing path for the PSI.

4. HSS determines the routing information, i.e., the address of the AS hosting the PSI.

5. HSS returns the AS address to the I-CSCF.

6-7. I-CSCF forwards the request to the address received from the query.

8-9. Session setup co[ntinues]~~mpletes~~ as per existing procedures.

Figure 5.4.12.b depicts an example routing scenario where the basic IMS routing via S-CSCF is used to route the session.

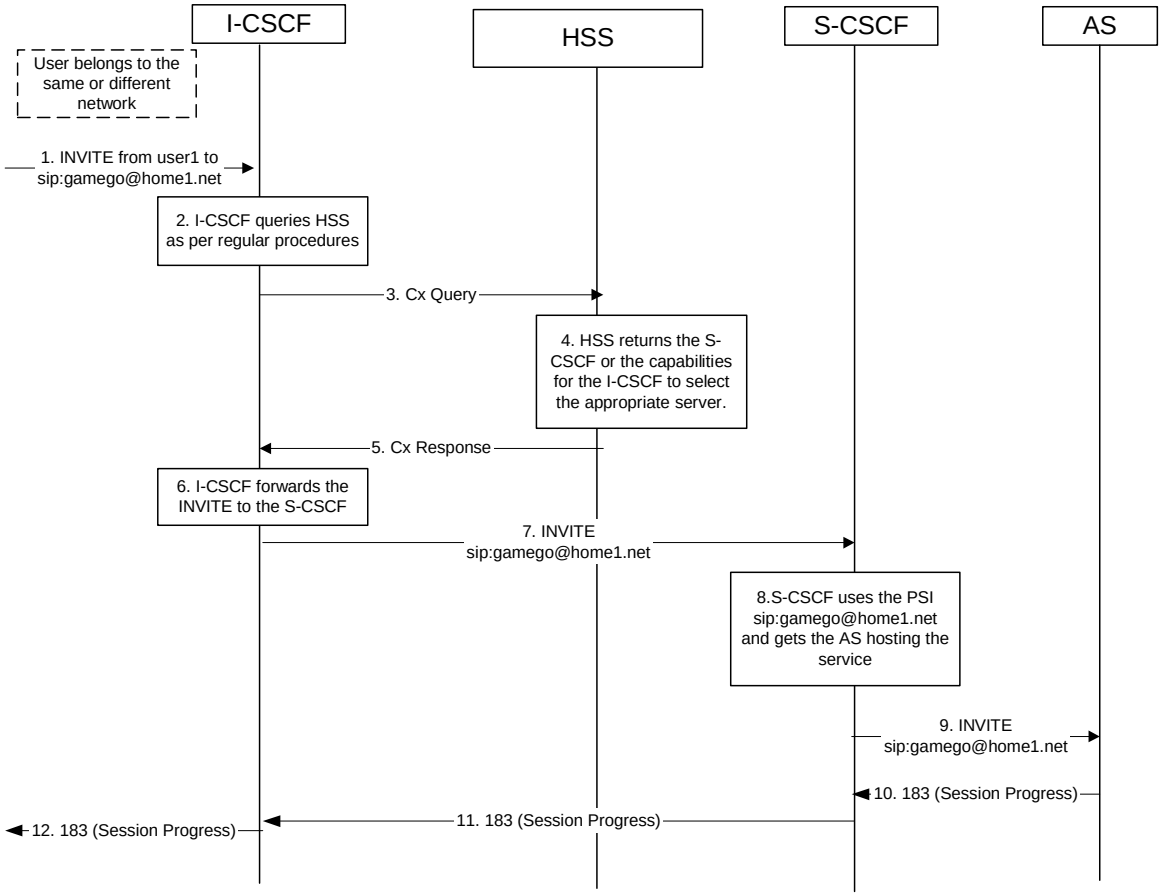


Figure 5.4.12.b Incoming session, indirect route to AS via S-CSCF

1. I-CSCF receives a request destined to the PSI.

2-3. I-CSCF queries HSS in order to determine the next hop in the routing path for the PSI.

4. HSS determines the routing information, which is the S-CSCF defined for the ~~AS hosting the PSI~~"PSI user".

5. HSS returns the S-CSCF address/capabilities to the I-CSCF.

6-7. I-CSCF, as per existing procedures, forwards the request towards the entity (i.e., S-CSCF) received from the query, or the I-CSCF selects a new S-CSCF if required.

8. S-CSCF evaluates the filter criteria and gets the AS address where to forward the request.

9. The request is then routed towards the AS identified by the filter criteria.

10-12. Session setup ~~completes~~ continues as per existing procedures.

5.4.12.3 Subdomain based PSIs ~~on the originating and terminating side~~

Subdomains defined for PSIs allow both operators and users to define specific ~~these~~ PSIs within subdomains for specific applications. For this purpose, subdomains ~~are~~ can be defined by the operator in the DNS infrastructure. ~~Within the subdomain, specific PSIs can be created either statically or dynamically.~~ Specific PSIs within a subdomain can be created and deleted by users using the Ut interface to the AS hosting the subdomain, or by the operator via O&M mechanisms.

Subdomain based PSIs are globally routable and can be made available to users within and outside the operator domain.

In this case, there are two ways to route towards the AS hosting the PSI:

a) When the subdomain name is defined in the global DNS, then the originating S-CSCF receives the IP address of the AS hosting the PSI, when it queries DNS. –The principles defined in RFC 3263 "Session Initiation Protocol (SIP): Locating SIP Servers" may be used. –For example, a NAPTR query and then a SRV query may be used to get the IP address of the AS.

b) The PSI is resolved by the global DNS to an I-CSCF address in the domain where the AS hosting the PSI is located. The I-CSCF recognises the subdomain (and thus does not query the HSS). It resolves the same PSI to the address of the actual destination AS hosting the PSI using an internal DNS mechanism, and forwards the requests directly to the AS.

Figure 5.4.12.c shows an example of DNS based routing of an incoming session from an external network. –The routing from the external network leads to the entry point of the IMS subsystem hosting the subdomain of the PSI.

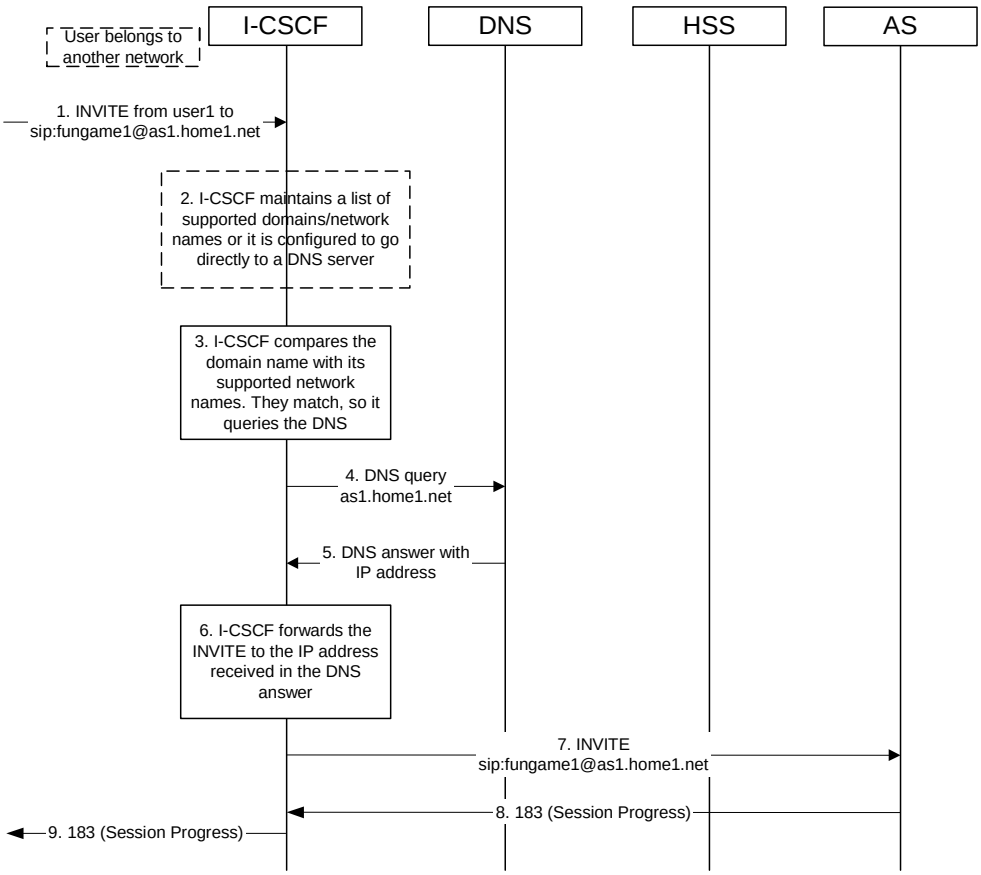


Figure 5.4.12.c Incoming session, direct route to AS using DNS

1. I-CSCF receives a request that is destined tothe PSI.
2. I-CSCF has been configured with the list of supported domains/network names, or it may have been configured to directly query a local DNS server.
3. In this case the I-CSCF checks the list and finds a match.
4. I-CSCF sends DNS query to find the route.
5. DNS server returns the IP address of the AS hosting the PSI.

6-7. I-CSCF forwards the request towards the IP address received from the query.

8-9. Session setup ~~completes~~ continues as per existing procedures.

5.4.12.4 PSI configuration in the HSS

In order to support configuration of an AS hosting a PSI ~~in the HSS~~, the distinct PSIs and/or wildcarded PSI ranges hosted in the AS need~~s~~ to be configured in the HSS. ~~This configuration is required when the PSI has S-CSCF assigned.~~ The configuration shall include procedures to allow:

- Distinct PSIs and wildcarded PSI ranges to be configured in the HSS via operation and maintanence procedures,
- ~~Allow a~~Authorization and verification of access as "PSI user" with the Public Service Identity ~~assigned to~~hosted by the AS, e.g. for AS-originating requests,
- ~~Allow a~~Access to "PSI user" information (e.g. the S-CSCF assigned) over the Cx reference point from the CSCF nodes,
- ~~Allow d~~Defining the "PSI user" similar to the principle of IMS user, without requiring any subscription/access information (e.g. CS/PS domain data) that are required for IMS user.

Further functional requirements such as how S-CSCF is provisioned with the PSI data need to be studied.

Note that the PSI configuration in the HSS does not affect the filter criteria based access to an AS as defined in the user profiles.

3GPP TSG-SA WG2 Meeting #38
Atlanta, USA, 16-20 February 2004

Tdoc ⌘S2-040974

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **395** ⌘**rev** **5** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Relation of IMS sessions and PDP Contexts
Source:	⌘	SA2 (Nokia)
Work item code:	⌘	IMS2
Date:	⌘	16/02/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	During the course of Rel5 development some mechanisms were introduced to allow the IMS network to control the groupping of media components to PDP Contexts. These mechanisms were put in place to ensure that appropriate charging can be performed with the underlying charging capabilities of Rel5 GPRS networks. In Rel6, a new feature is being introduced that enables operators to use IP flow-based charging capabilities on the bearer level, e.g. in GPRS. In networks that implement this new functionalilty, the IMS-based control mechanism developped in Rel5 becomes unnecessary.
Summary of change:	⌘	The IMS level control for media groupping is kept as an optional mechanism for backwards compatibility mainly. Additionally, the restriction of bundling IMS media components from different IMS sessions to the same PDP Context is removed.
Consequences if not approved:	⌘	

Clauses affected:	⌘	E.2.2.1			
Other specs Affected:	⌘	**Y** / **N**	Other core specifications	⌘	23.207
		X /	Other core specifications		
		/ **X**	Test specifications		
		/ **X**	O&M Specifications		
Other comments:	⌘				

How to create CRs using this form:

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

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

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

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

*** FIRST AND ONLY CHANGE ***

E.2.2.1 Relation of IMS media components and PDP contexts carrying IMS media

The relation between IMS media components and PDP contexts carrying IMS media ~~is~~ may be controlled by the IMS network on media component level in the following way:

The P-CSCF ~~shall have the capability to~~ indicates to the UE that a separate PDP Context is required for each IMS media component indicated.The P-CSCF shall apply and maintain the same policy to separate specific media components into separate PDP Contexts during a session. If a media component is added during the session, the new decision on the separation for the media components shall not contradict any former decisions. For mobile originating sessions the P-CSCF shall apply the policy to the initial offer to ensure identical decisions for different answers, e.g. a media component not required to use a separate PDP Context initially, shall not later require a separate PDP Context (e.g. in case of subsequent answers received due to forking).

- If the UE receives such an indication for a media component, it shall open a separate PDP Context for this media component.

- If the UE receives no such indication for a media component, the UE makes the decision whether to open a separate PDP Context or modify an existing PDP Context for this media component. In this case, the UE may also decide to carry media components from different IMS sessions in the same PDP context, as long as none of the bundled media components is required to be kept separate.

- The criteria and information for setting this indication is determined by local policy in the network where the P-CSCF is located.

  Note: the Flow-based bearer charging capabilities of the P-CSCF's network, and the capabilities of deployed UEs should be taken into account when defining such policies in the visited IMS network operator's domain.

- The IMS network shall have the capability to transfer the media component level indication described above to the UE. It shall be possible to ~~This media component level indication shall be~~ transfer~~red~~ this media component level indication in SIP/SDP signaling upon session initiation and addition of media component(s) to active IMS sessions.

~~It is assumed that media components from different IMS sessions are not carried within the same PDP context.~~

All associated IP flows (such as e.g. RTP / RTCP flows) used by the UE to support a single media component are assumed to be carried within the same PDP context.

3GPP TSG-SA WG2 Meeting #37 **Tdoc ⌘S2-040401**
Innsbruck, Austria, 12th – 16th January 2004.

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **396** ⌘**rev** **1** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Support for Caller preferences
Source:	⌘	SA2 (Ericsson)
Work item code:	⌘	IMS2
Date:	⌘	14/01/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	It is already possible to register the capabilities and characteristics of the SIP UA during the IMS registration, but it is not defined how that information can be used during session set-up.
Summary of change:	⌘	It is proposed to add the support for caller preferences according to draft-ietf-sip-callerprefs-10, i.e. a SIP request may also contain preferences for characteristics of the SIP UA that is to be reached. If such preferences are included and the characteristics are previously registered by the UE then the S-CSCF shall follow the preference matching as specified in “draft-ietf-sip-callerprefs-10”. It is also clarified that draft-ietf-sip-callerprefs-10 is used when adding preference related to forking.
Consequences if not approved:	⌘	

Clauses affected:	⌘	2, 4.2.7.3, 4.6.3			
Other specs affected:	⌘	Y: X / N:	Other core specifications	⌘	24.229
		Y: / N: X	Test specifications		
		Y: / N: X	O&M Specifications		
Other comments:	⌘				

How to create CRs using this form:

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

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

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

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

********** First Change**********

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 TS 23.002: "Network Architecture".

[2] CCITT Recommendation E.164: "Numbering plan for the ISDN era".

[3] CCITT Recommendation Q.65: "Methodology – Stage 2 of the method for the characterisation of services supported by an ISDN".

[4] ITU Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN"

[5] GSM 03.64: "Digital cellular telecommunication system (Phase 2+); Overall Description of the General Packet Radio Service (GPRS) Radio Interface; Stage 2".

[6] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[7] 3GPP TS 23.221: "Architectural Requirements".

[8] 3GPP TS 22.228: "Service requirements for the IP multimedia core network subsystem"

[9] 3GPP TS 23.207: "End-to-end QoS concept and architecture"

[10] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP"

[10a] 3GPP TS 24.229: " IP Multimedia Call Control based on SIP and SDP; Stage 3"

[11] 3GPP TS 25.301: "Radio interface protocol architecture"

[11a] 3GPP TS 29.207: " Policy control over Go interface "

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

[13] RFC 2396: "Uniform Resource Identifiers (URI): Generic Syntax"

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

[15] RFC 2806: "URLs for Telephone Calls"

[16] RFC 2916: "E.164 number and DNS"

[16a] RFC 3041: "Privacy Extensions for Stateless Address Autoconfiguration in IPv6"

[17] ITU Recommendation G.711: "Pulse code modulation (PCM) of voice frequencies"

[18] ITU Recommendation H.248: "Gateway control protocol"

[19] 3GPP TS 33.203: "Access Security for IP-based services"

[20] 3GPP TS 33.210: "Network Domain Security: IP network layer security "

[21] 3GPP TS 26.235: "Packet Switched Multimedia Applications; Default Codecs".

[22] 3GPP TR 22.941: " IP Based Multimedia Services Framework "

[23] 3GPP TS 23.060: “General Packet Radio Service (GPRS); Service description; Stage 2

[24] 3GPP TS 23.003: “Technical Specification Group Core Network; Numbering, addressing and identification”

[25] 3GPP TS 32.200: “Telecommunication management; Charging management; Charging principles”

[26] 3GPP TS 32.225: ” Telecommunication Management; Charging Management; Charging Data Description for IP Multimedia Subsystem”

[27] 3GPP TS 22.071: “Technical Specification Group Services and System Aspects,Location Services (LCS);Service description, Stage 1”

[28] 3GPP TS 23.271: “Technical Specification Group Services and System Aspects, Functional stage 2 description of LCS”

[29] 3GPP TS 23.078: “Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 3 - Stage 2”

[29a] 3GPP TS 22.340: “ IMS Messaging; Stage 1”

[30] 3GPP TS 29.228:“IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents”

[31] 3GPP TS 23.240: "3GPP Generic User Profile - Architecture; Stage 2"

[32] 3GPP TS 22.250: “IP Multimedia Subsystem (IMS) group management”; Stage 1”

[33] RFC 2766: “Network Address Translation-Protocol Translation (NAT-PT)”

[34] RFC 2663: “IP Network Address Translator (NAT) Terminology and Considerations”

[35] Transition Scenarios for 3GPP Networks, draft-ietf-v6ops-3gpp-cases-03.txt, work in progress

[36] 3GPP TS 23.141: “Technical Specification Group Services and System Aspects, Presence Service”

[37] 3GPP TS 26.xxx:” IMS messaging and Presence; Media formats and codecs”

[38] draft-ietf-sip-callee-caps-01 (October 2003): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"

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

[39] IETF RFC 3323 (2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[40] IETF RFC 3325 (2002): "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Network".

[y] draft-ietf-sip-callerprefs-10 (October 2003): "Caller Preferences for the Session Initiation Protocol (SIP)”

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

********** Second Change**********

4.2.7 Support of SIP forking

4.2.7.1 SIP Forking

SIP forking is the ability of a SIP proxy server to fork SIP request messages to multiple destinations according to RFC 3261 [12].

4.2.7.2 Forking within and outside the IM CN Subsystem

The IM CN subsystem shall have the capability to fork requests to multiple destinations; this capability is subject to rules for forking proxies defined in RFC 3261 [12].

- The S-CSCF shall support the ability for a public user identity to be registered from multiple contact addresses, as defined in RFC 3261 [12]. The S-CSCF shall support forking so that an incoming SIP request addressed to a Public User Identity is proxied to multiple registered contact addresses. This allows forking across multiple contact addresses of the same Public User Identity.

- When multiple contact addresses have been registered, then the S-CSCF shall fork the incoming SIP request. If the UE has indicated preference information upon registration, then the S-CSCF shall use it to decide if parallel or sequential forking is used, as described in RFC 3261 [12]. If the UE has not indicated any preference for the contact addresses upon registration, or if the preferences for the contact addresses have equal value, then it is up to the S-CSCF if parallel or sequential forking is to be performed.

- Application Servers in the IMS may act as a forking proxy in the sense of RFC 3261 [12] and may fork a SIP request across multiple Public User Identities allocated to the same user. S-CSCFs shall provide the necessary support for forking by Application Servers.

Additionally, other networks outside the IM CN Subsystem are able to perform SIP forking.

4.2.7.3 Support for forked requests

UE and MGCF shall be ready to receive responses generated due to a forked request and behave according to the procedures specified in [12] and in this section.

The UE and MGCF may accept or reject early dialogues from different terminations as described in [12], for example if the UE is only capable of supporting a limited number of simultaneous dialogs.

Upon the reception of a first final 200 OK (for INVITE), the UE or MGCF shall acknowledge the 200 OK and cancel other early dialogues that may have been established. In this case the UE or MGCF may require updating the allocated resources according to the resources needed. In case it receives a subsequent 200 OK, the UE or MGCF shall acknowledge the dialogue and immediately send a BYE to drop the dialog.

The UE and MGCF may include preferences according to “draft-ietf-sip-callerprefs-10” [y], in INVITE's, indicating that proxies should not fork the INVITE request. The S-CSCF and AS should follow the preferences, if included in the INVITE request.

On the terminating side, UE and MGCF shall be able to receive, as specified in [12], several requests for the same dialog that were forked by a previous SIP entity.

Application Servers and MRFCs shall be capable to handle forked requests according to the procedures specified in [12].

********** Third Change**********

4.6.3 Serving-CSCF

The Serving-CSCF (S-CSCF) performs the session control services for the UE. It maintains a session state as needed by the network operator for support of the services. Within an operator's network, different S-CSCFs may have different functionalities. The functions performed by the S-CSCF during a session are:

Registration

- May behave as a Registrar as defined in RFC 3261 [12] or subsequent versions, i.e. it accepts registration requests and makes its information available through the location server (eg. HSS).

Session-related and session-unrelated flows

- Session control for the registered endpoint's sessions. It shall reject IMS communication to/from public user identity(s) that are barred for IMS communications after completion of registration, as described in subclause 5.2.1.
- May behave as a Proxy Server as defined in RFC 3261 [12] or subsequent versions, i.e. it accepts requests and services them internally or forwards them on, possibly after translation.
- May behave as a User Agent as defined in RFC 3261 [12] or subsequent versions, i.e. it may terminate and independently generate SIP transactions.
- Interaction with Services Platforms for the support of Services
- Provide endpoints with service event related information (e.g. notification of tones/announcement together with location of additional media resources, billing notification)
- On behalf of an originating endpoint (i.e. the originating user/UE)
  - Obtain from a database the Address of the I-CSCF for the network operator serving the destination user from the destination name (e.g. dialled phone number or SIP URL), when the destination user is a customer of a different network operator, and forward the SIP request or response to that I-CSCF.
  - When the destination name of the destination user (e.g. dialled phone number or SIP URL), and the originating user is a customer of the same network operator, forward the SIP request or response to an I-CSCF within the operator's network.
  - Depending on operator policy, forward the SIP request or response to another SIP server located within an ISP domain outside of the IM CN subsystem.
  - Forward the SIP request or response to a BGCF for call routing to the PSTN or CS Domain.
- On behalf of a destination endpoint (i.e. the terminating user/UE)
  - Forward the SIP request or response to a P-CSCF for a MT procedure to a home user within the home network, or for a user roaming within a visited network where the home network operator has chosen not to have an I-CSCF in the path
  - Forward the SIP request or response to an I-CSCF for a MT procedure for a roaming user within a visited network where the home network operator has chosen to have an I-CSCF in the path.
  - Modify the SIP request for routing an incoming session to CS domain according to HSS and service control interactions, in case the user is to receive the incoming session via the CS domain.
  - Forward the SIP request or response to a BGCF for call routing to the PSTN or the CS domain.
  - If the SIP request contains preferences for characteristics of the destination endpoint, perform preference and capability matching as specified in "draft-ietf-sip-callerprefs-10" [y].

Charging and resource utilisation:

- Generation of CDRs

********** End of Change**********

3GPP TSG-SA WG2 Meeting #37 **Tdoc ⌘S2-040937**
Innsbruck, Austria, 12th – 16th January 2004.

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **397** ⌘**rev** **3** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Message size limitations for Immediate messaging
Source:	⌘	SA2 (Ericsson, Nokia)
Work item code:	⌘	IMS2
Date:	⌘	14/01/2004
Category:	⌘	**C**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	For immediate messaging the user traffic will traverse the same path as any session control requests, whereas session based messaging uses a separate path for the user traffic. The UE could decide to use immediate messaging, i.e. SIP MESSAGE, when sending large content. To avoid the negative effects of sending large amount of user traffic in the session control path it would be desirable to use alternative means to transfer the large content.
Summary of change:	⌘	It is proposed that if the message size exceeds the size limit for MESSAGE requests, the UE shall use alternative means to deliver the content of the Immediate Message.
Consequences if not approved:	⌘	

Clauses affected:	⌘	2, 5.16.1.1

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		24.229
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

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

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

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

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

********** First Change**********

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 TS 23.002: "Network Architecture".

[2] CCITT Recommendation E.164: "Numbering plan for the ISDN era".

[3] CCITT Recommendation Q.65: "Methodology – Stage 2 of the method for the characterisation of services supported by an ISDN".

[4] ITU Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN"

[5] GSM 03.64: "Digital cellular telecommunication system (Phase 2+); Overall Description of the General Packet Radio Service (GPRS) Radio Interface; Stage 2".

[6] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[7] 3GPP TS 23.221: "Architectural Requirements".

[8] 3GPP TS 22.228: "Service requirements for the IP multimedia core network subsystem"

[9] 3GPP TS 23.207: "End-to-end QoS concept and architecture"

[10] 3GPP TS 24.228: "Signalling flows for the IP multimedia call control based on SIP and SDP"

[10a] 3GPP TS 24.229: " IP Multimedia Call Control based on SIP and SDP; Stage 3"

[11] 3GPP TS 25.301: "Radio interface protocol architecture"

[11a] 3GPP TS 29.207: " Policy control over Go interface "

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

[13] RFC 2396: "Uniform Resource Identifiers (URI): Generic Syntax"

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

[15] RFC 2806: "URLs for Telephone Calls"

[16] RFC 2916: "E.164 number and DNS"

[16a] RFC 3041: "Privacy Extensions for Stateless Address Autoconfiguration in IPv6"

[17] ITU Recommendation G.711: "Pulse code modulation (PCM) of voice frequencies"

[18] ITU Recommendation H.248: "Gateway control protocol"

[19] 3GPP TS 33.203: "Access Security for IP-based services"

[20] 3GPP TS 33.210: "Network Domain Security: IP network layer security "

[21] 3GPP TS 26.235: "Packet Switched Multimedia Applications; Default Codecs".

[22] 3GPP TR 22.941: " IP Based Multimedia Services Framework "

[23] 3GPP TS 23.060: “General Packet Radio Service (GPRS); Service description; Stage 2

[24] 3GPP TS 23.003: “Technical Specification Group Core Network; Numbering, addressing and identification”

[25] 3GPP TS 32.200: “Telecommunication management; Charging management; Charging principles”

[26] 3GPP TS 32.225: ” Telecommunication Management; Charging Management; Charging Data Description for IP Multimedia Subsystem”

[27] 3GPP TS 22.071: “Technical Specification Group Services and System Aspects,Location Services (LCS);Service description, Stage 1”

[28] 3GPP TS 23.271: “Technical Specification Group Services and System Aspects, Functional stage 2 description of LCS”

[29] 3GPP TS 23.078: “Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 3 - Stage 2”

[29a] 3GPP TS 22.340: “ IMS Messaging; Stage 1”

[30] 3GPP TS 29.228:“IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents”

[31] 3GPP TS 23.240: "3GPP Generic User Profile - Architecture; Stage 2"

[32] 3GPP TS 22.250: “IP Multimedia Subsystem (IMS) group management”; Stage 1”

[33] RFC 2766: “Network Address Translation-Protocol Translation (NAT-PT)”

[34] RFC 2663: “IP Network Address Translator (NAT) Terminology and Considerations”

[35] Transition Scenarios for 3GPP Networks, draft-ietf-v6ops-3gpp-cases-03.txt, work in progress

[36] 3GPP TS 23.141: “Technical Specification Group Services and System Aspects, Presence Service”

[37] 3GPP TS 26.xxx:” IMS messaging and Presence; Media formats and codecs”

[38] draft-ietf-sip-callee-caps-01 (October 2003): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"

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

[39] IETF RFC 3323 (2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[40] IETF RFC 3325 (2002): "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Network".

[xx] IETF RFC 3428 (2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

********** Second Change**********

5.16 IMS messaging concepts and procedures

This clause describes architectural concepts and procedures for providing Messaging in the IM CN Subsystem. The service enablers for Messaging and possible reuse of IMS service enablers within this context as well security and

charging expectations, addressing, privacy, content handling and limitations, filtering, media types and message lengths, etc. are to be further studied.

Any ISIM related architectural requirements would be studied as part of overall IMS Messaging.

5.16.1 Immediate Messaging

This sub-clause describes architectural concepts and procedures for fulfiling the requirements for Immediate Messaging described in TS 22.340 [29a].

5.16.1.1 Procedures to enable Immediate Messaging

IMS users shall be able to exchange immediate messages with each other by using the procedure described in this sub-clause. This procedure shall allow the exchange of any type of multimedia content (subject to possible restrictions based on operator policy and user preferences/intent), for example but not limited to:

- Pictures, video clips, sound clips with a format defined by 3GPP TS 26.xxx [37]

If the message size exceeds the size limit for MESSAGE requests, the UE shall use alternative means to deliver the content of the Immediate Message. Session based messaging specified in subclause 5.16.2 provides such means. RFC 3428[xx] presents guidelines for the selection of transport mechanism for an Immediate Message. The message size limitations described above are meant to be applicable for Immediate Messages sent over end-to-end congestion safe transport, i.e. are not necessarily equal to the limitations specified for MESSAGE over congestion-unsafe transport by RFC 3428 [xx].

Note: The actual size limit is part of stage-3 design.

If the size limit for a terminating MESSAGE request is exceeded, the network may refuse the request or respond to the sender with an indication that the size of the message is too large.

The sender UE can include an indication in the message regarding the length of time the message will be considered valid.

5.16.1.1.1 Immediate messaging procedure to registered public user identity

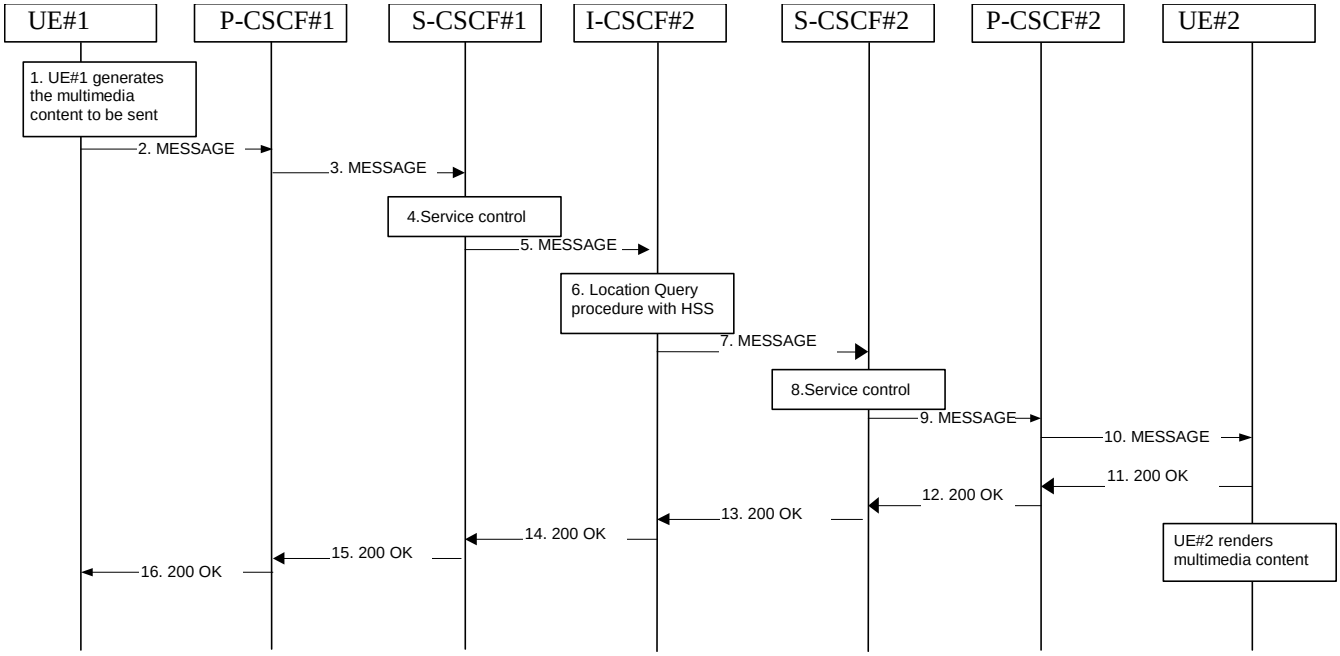


Figure 5.47: Immediate Messaging procedure to registered public user identity

1. UE#1 generates the multimedia content intended to be sent to UE#2.

2. UE#1 sends the MESSAGE request to P-CSCF#1 that includes the multimedia content in the message body.
3. P-CSCF#1 forwards the MESSAGE request to S-CSCF#1 along the path determined upon UE#1's most recent registration procedure.
4. Based on operator policy S-CSCF#1 may reject the MESSAGE request with an appropriate response, e.g. if content length or content type of the MESSAGE are not acceptable. S-CSCF#1 invokes whatever service control logic is appropriate for this MESSAGE request. This may include routing the MESSAGE request to an application server, which processes the request further on.
5. S-CSC#1 forwards the MESSAGE request to I-CSCF#2.
6. I-CSCF#2 performs Location Query procedure with the HSS to acquire the S-CSCF address of the destination user (S-CSCF#2).
7. I-CSCF#2 forwards the MESSAGE request to S-CSCF#2.
8. Based on operator policy S-CSCF#2 may reject the MESSAGE request with an appropriate response, e.g. if content length or content type of the MESSAGE are not acceptable. S-CSCF#2 invokes whatever service control logic is appropriate for this MESSAGE request. This may include routing the MESSAGE request to an application server, which processes the request further on.
   For example, the UE#2 may have a service activated that blocks the delivery of incoming messages that fullfill criterias set by the user. The AS may then respond to the MESSAGE request with an appropriate error response.
9. S-CSCF#2 forwards the MESSAGE request to P-CSCF#2 along the path determined upon UE#2's most recent registration procedure.
10. P-CSCF#2 forwards the MESSAGE request to UE#2. After receiving the MESSAGE UE#2 renders the multimedia content to the user.
11. – 16. UE#2 acknowledges the MESSAGE request with a response that indicates that the destination entity has received the MESSAGE request. The response traverses the transaction path back to UE#1.

5.16.1.1.2 Immediate messaging procedure to unregistered public user identity

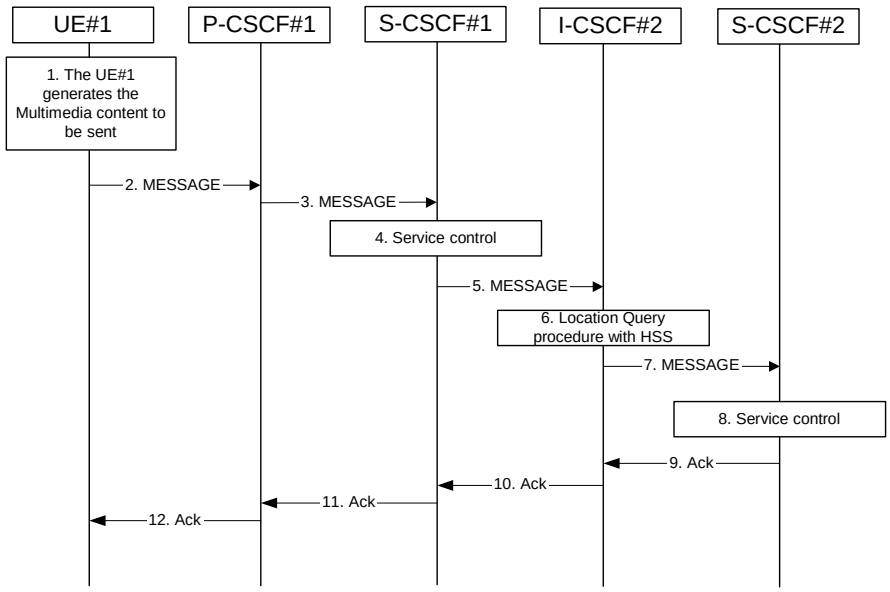


Figure 5.48: Immediate messaging to unregistered public user identity, service control invoked

1-5. The same actions apply as for when the Public user identity is registered, see step 1-5 in clause 5.16.1.1.1.

6. I-CSCF#2 interacts with the HSS as per the terminating procedures defined for unregistered public user identities in clause 5.12.1. If the public user identity has no services related to unregistered state activated the interaction with HSS would be as per the procedure defined in clause 5.12.2.

7. I-CSCF#2 forwards the MESSAGE request to S-CSCF#2.

8. Based on operator policy S-CSCF#2 may reject the MESSAGE request with an appropriate response, e.g. if content length or content type of the MESSAGE are not acceptable or the UE#2 does not have a service activated that temporarily hold the MESSAGE request in the network.

S-CSCF#2 invokes whatever service control logic appropriate for this MESSAGE request. This may include routing the MESSAGE request to an application server, which processes the request further on.

For example, the UE#2 may have a service activated that allows delivery of any pending MESSAGE request. The AS may then hold the MESSAGE request and deliver the MESSAGE request when the UE#2 becomes reachable. In this case, depending on user settings UE#2 controls the delivery of the pending MESSAGEs.

9-12. The MESSAGE request is acknowledged with an appropriate acknowledgement response. The acknowledgement response traverses the transaction path back to UE#1.

5.16.1.2 Immediate messages with multiple recipients

IMS users shall be able to send a single immediate message to multiple recipients, as specified in 3GPP TS 22.340 [29a]. The following means are supported to achieve this:

- A PSI identifying a new group is created in the appropriate Application Server, and members are added to this group (e.g. by the user via the Ut interface or by the operator via O&M mechanisms). Immediate messages addressed to this PSI will be routed to the AS hosting the PSI, and this AS shall create and send immediate messages addressed to a group member of the group identified by the PSI.

- The user can send an immediate message by indicating the individual addresses (Public User Identities for IMS recipients) of the intended recipients as part of the immediate message. The AS of the user shall then create and send immediate messages addressed to each one of the intended recipients.

5.16.2 Session-based Messaging

This subclause describes architectural concepts and procedures for fulfiling the requirements for Session-based Messaging described in TS 22.340 [29a].

5.16.2.1 Architectural principles

Session-based IMS messaging communications shall as much as possible use the same basic IMS session delivery mechanisms (e.g. routing, security, service control) as defined in clause 4 and 5 of this document. For session based messaging the session shall include a messaging media component, other media components may also be included. Once the session containing a messaging media component is established, messages in the session are transported between the session participants as per the parameters defined in the messaging media component part of the session description (SDP).

For addressing chat-group-type session based messaging the concept of Public Service Identities is used.

Session based messaging is available for users that are registered in the IMS.

The session based messaging shall be able to provide the following functionality:

-Per-message-based charging, as well as content- and size-based charging.

-Operator-controlled policy to be set on the size and content of the messages.

-Support for a messaging media component as part of a session where other media components are also included.

-Support for messaging-only sessions.

5.16.2.2 Procedures to enable Session based Messaging

IMS users shall be able to exchange session-based messages with each other by using the procedure described in this sub-clause. This procedure shall allow the exchange of any type of multimedia content (subject to possible restrictions based on operator policy and user preferences/intent), for example but not limited to:

- Pictures, video clips, sound clips with a format defined by 3GPP TS 26.xxx [37]

5.16.2.2.1 Session based messaging procedure to registered public user identity

Editor's note: This sub-clause will describe session based messaging between two UEs.

5.16.2.2.2 Session based messaging procedure using multiple UEs

Editor's note: This sub-clause will describe session based messaging between multiple UEs using for example a Chat session.

********** End of Change**********

3GPP TSG-SA WG2 Meeting #38
Atlanta, USA, 16th – 20th February 2004

Tdoc ⌘S2-040938

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **398** ⌘**rev** **4** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Session based messaging requirements and flows
Source:	⌘	SA2 (Ericsson, Siemens)
Work item code:	⌘	IMS2
Date:	⌘	18/02/2004
Category:	⌘	**B**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	The section for session based messaging is not completed. It has been agreed that preconditions should be avoided for session based messaging due to the undesireable amount of extra signalling. SA2#37 agreed that message conferences are hosted either on a MRFC/MRFP or an IMS AS. In the first case however it is not clear how an UE can manage the conference parameters at the MRFC in a simple way. We propose therefore that the MRFC may be co-located with an AS for that purpose as it is already the working assumption in CN1 for conferencing.
Summary of change:	⌘	Flows for session based messaging are added and the role of the MRFC/MRFP and AS is clarified. If a MRFC/MRFP hosts session based messaging conferences, the MRFC may be co-located with an AS in order to enable the UE managing information related to the messaging conference.
Consequences if not approved:	⌘	It is unclear how messaging conferences can be managed by the user, if a MRFC/MRFP is used as message conferencing server.

Clauses affected:	⌘	5.16.2.2.2

Other specs affected: ⌘	Y	N		⌘	
	X		Other core specifications	⌘	24.229
		X	Test specifications		
		X	O&M Specifications		

Other comments:	⌘	

How to create CRs using this form:

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

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

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

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

********** First Change**********

5.16.2.2.2 Session based messaging procedure using multiple UEs

~~Editor's note: This sub-clause will describe session based messaging between multiple UEs using for example a Chat session.~~

Session based messaging between more than two UEs require the establishment of a session based messaging conference.

Within session based messaging conferences including multiple UEs (e.g. multiparty chat conferences) an MRFC/MRFP or an IMS AS shall be used to control the media resources.

When MRFC/MRFP are used, then conferencing principles are used to provide the chat service:

- MRFP must be able to establish message connections with all involved parties.
- MRFC/MRFP must be able to receive messages from conference participants and to distribute messages to all or some of the participants.
- In order to enable the UE managing information related to the session based messaging conference the MRFC may be co-located with an IMS AS.
- MRFC/MRFP roles and interactions with an AS are described in more detail in chapters 4.7 and 5.14.1 and 5.14.2.
- The interface for session based messaging between MRFC and MRFP is not standardised in this release.

When an AS is used, then the IMS service control architecture is used to provide the chat service. Both signalling and user plane are then supported by the AS. For more details, see section 4.2.

The following flow shows the originating session based messaging set up using an intermediate server for a chat service. In this case the intermediate chat server is addressesed by the UE#1 using a PSI. It is assumed that UE#1 is the first UE entering the chat session.

NOTE: Interactions between MRFC and MRFP are not shown in the flows below since these interactions are not standardized.

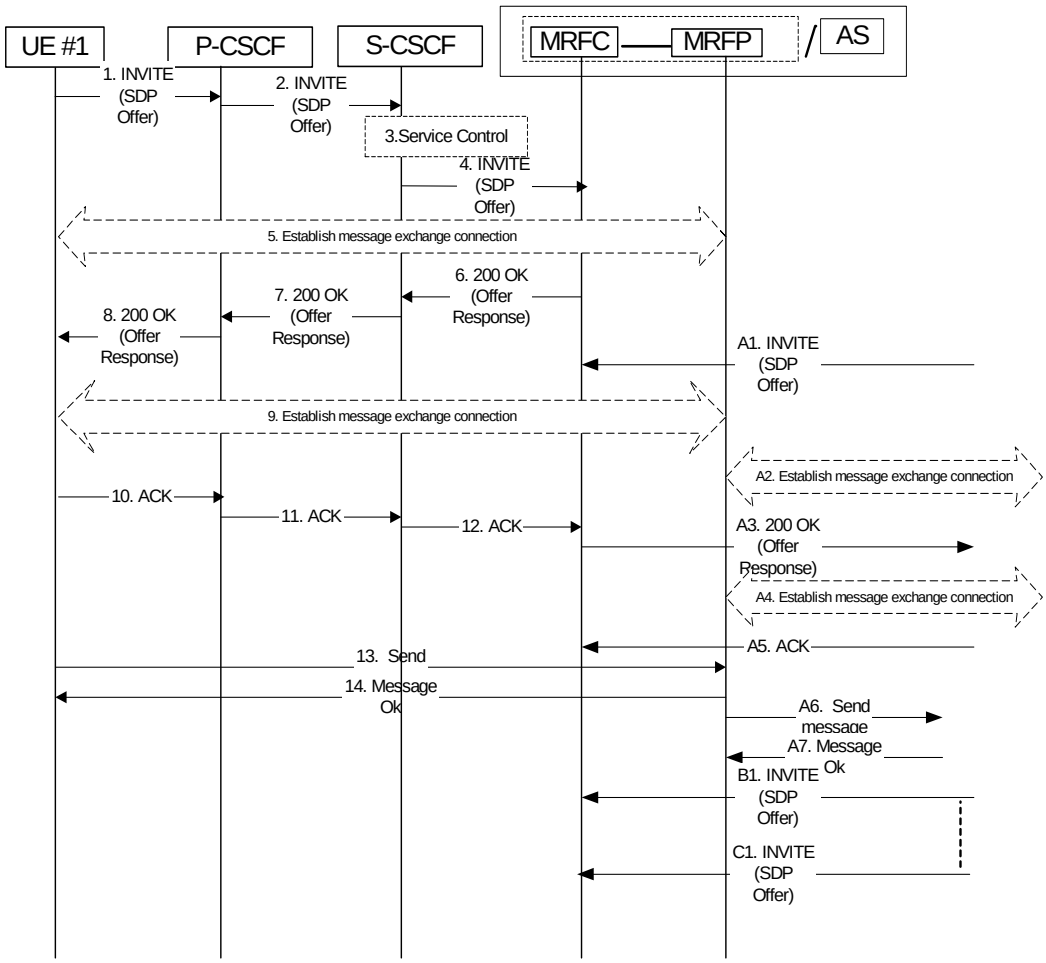


Figure x: Session based messaging using a chat server

1. UE #1 generates and sends an INVITE request addressed to a conferencing or chat PSI. The SDP offer indicates that UE#1 wants to establish a message session and contains all necessary information to do that.

2. P-CSCF forwards the INVITE to S-CSCF that then forwards the INVITE to the MRFC (~~/~~AS).

3. S-CSCF#1 may invoke service control for UE#1.

4. S-CSCF forwards the INVITE request to the MRFC/AS.

5. Since in this case the MRFP/AS hosts the session, the connection establishment towards UE#1 for exchange of the message media is not performed at this time.

6-8. MRFC/AS acknowledges the INVITE.

9. MRFP/AS establishes reliable end –to-end connection for exchange of the message media.

10-12. UE#1 acknowledges the establishment of the messaging session.

13. UE#1 sends a message towards the MRFP/AS.

14. MRFP/AS acknowledges the message

A1. Another UE sends an INVITE request addressed to the same conferencing or chat PSI. The initial SDP indicates that the UE wants to establish a message session and contains all necessary information to do that

A2. MRFP/AS hosts the session and the connection is not established at this point if the UE#2 also offers to host the session in its response.

A3. MRFC/AS acknowledges the INVITE

A4. MRFP/AS initiates the establishment of a messaging path connection towards the UE#2.

A5. UE#2 acknowledges the establishment of the session.

A6-A7. MRFP/AS forwards the message to all recipients e.g. all in the chat room.

B1-C1. INVITE requests (i.e. from new possible participants to the session) may arrive at any time.

Further messages may be exchanged in either direction between UEs using the established connection via the MRFC/MRFP or AS.

********** End of Change**********

3GPP TSG-SA WG2 Meeting #37
Innsbruck, Austria, 12-16 January 2004

Tdoc ⌘S2-040403

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **399** ⌘**rev** **1** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Reference to Local Services in chapter 4.3.3.3a of 23.228
Source:	⌘	SA2 (Siemens)
Work item code:	⌘	IMS2
Date:	⌘	30/12/2003
Category:	⌘	**D**
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	In chapter 4.3.3.3a of 23.228 it is stated that support of local services and local dialling plans is not specified in the document. This is not correct with respect to local services as these services are specified in chapter 4.2.2 of 23.228.
Summary of change:	⌘	Remove the reference to local services as not specified feature in 23.228.
Consequences if not approved:	⌘	Inconsistent text in chapters 4.2.2 and 4.3.3.3a of 23.228.

Clauses affected:	⌘	4.3.3.3a			
Other specs affected:	⌘	**Y**	**N**		⌘
			X	Other core specifications	
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

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

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

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

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

********** MODIFIED SECTION **********

4.3.3.3a Handling of dialled number formats

When using a phone number as the dialled address, the UE can provide this number in the form of a SIP URI or a TEL URL. This phone number can be in the form of E.164 format (prefixed with a '+' sign), or a local format using local dialling plan and prefix. The IMS will interpret the phone number with a leading '+' to be a fully defined international number.

~~Support for local services and of local dialling plans areis not specified in the present document.~~

3GPP TSG-SA2 Meeting #38
Atlanta, USA, 2004.02.16-20

Tdoc ⌘S2-040942
rev of S2-040782

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **403** ⌘**rev** **1** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Proposed clarifications to MRFC/MRFP
Source:	⌘	SA2 (Convedia)
Work item code:	⌘	IMS2
Date:	⌘	2004 02 17
Category:	⌘	**C**
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	Resolve existing minor issues with the role of the MRF.
Summary of change:	⌘	Correction to the wording for the role of the MRF.
Consequences if not approved:	⌘	Minor confusion in role of MRF.

Clauses affected:	⌘	4.7

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

Other comments: ⌘

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

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

4.7 Multimedia Resource Function

The architecture concerning the Multimedia Resource Function is presented in Figure 4.5a below.

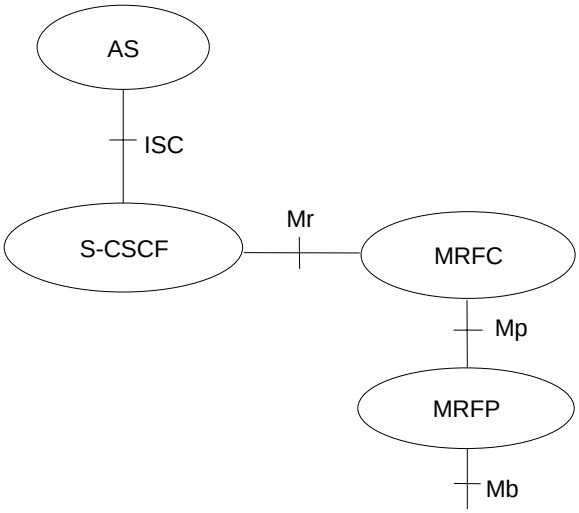


Figure 4.5a: Architecture of MRF

The MRF is split into Multimedia Resource Function Controller (MRFC) and Multimedia Resource Function Processor (MRFP).

Tasks of the MRFC are the following:

- Control the media stream resources in the MRFP.
- Interpret information coming from an AS and S-CSCF (e.g session identifier) and control MRFP accordingly.
- Generate of CDRs.

Tasks of the MRFP ~~are~~ include the following:

- Control of the bearer on the Mb reference point.
- Provide resources to be controlled by the MRFC.
- Mixing of incoming media streams (e.g for multiple parties).
- Media stream source (for multimedia announcements).
- Media stream processing (e.g. audio transcoding, media analysis).

Tasks of an Application Server with regards to MRF are e.g. the following:

- Conference booking and ~~provide~~ management of booking information (e.g. start time, duration, list of participants) ~~to the MRFC~~.
- Provide a floor control mechanism, by which end users (e.g. participants, chairman) can influence floor and provide information to the MRFC on how incoming media streams should be mixed and distributed accordingly.

The protocol used for the Mr reference point is SIP (as defined by RFC 3261 [12], other relevant RFC's, and additional enhancements introduced to support 3GPP´s needs).

The Mp reference point allows an MRFC to control media stream resources provided by an MRFP.

The Mp reference point has the following properties:

- Full compliance with the H.248 standard.
- Open architecture where extensions (packages) definition work on the interface may be carried out.

The protocol for the Mp reference point is not specified in this release.

---END---

3GPP TSG-SA WG2 Meeting #38
Atlanta, 16-20 February 2004

Tdoc ⌘S2-040943

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **404** ⌘**rev** **1** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Relationship between private user IDs and IMS subscription
Source:	⌘	SA2 (Lucent Technologies)
Work item code:	⌘	IMS2
Date:	⌘	16/02/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	It is not currently clear whether one subscription can contain multiple private user IDs although the text seems to imply this capability.
Summary of change:	⌘	Clarify the figures and text to indicate that an IMS subscription can contain multiple private user IDs. Also incorrect figure numbering has been corrected.
Consequences if not approved:	⌘	Implementation at stage-3 may not account for this configuration.

Clauses affected:	⌘	4.3.3.4, 4.7, and 5.2.1a

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

⌘

Other comments: ⌘

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

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

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

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

***** First Change *****

4.3.3.4 Relationship of private and public user identities

The home network operator is responsible for the assignment of the private user identifier, and public user identifiers; other identities that are not defined by the operator may also exist.

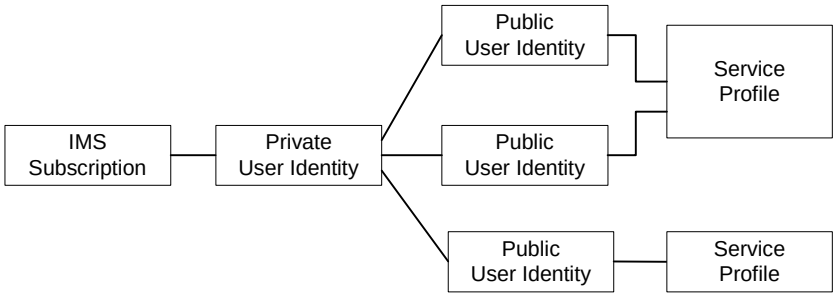


Figure 4.5: Relationship of the private user identity and public user identities

The IMS Service Profile is a collection of service and user related data as defined in 3GPP TS 29.228 [30]. The Service Profile is independent from the Implicit Registration Set, e.g. IMPUs with different Service Profiles may belong to the same Implicit Registration Set. Initial filter criteria in the service profile provide a simple service logic comprising of user / operator preferences that are of static nature i.e. they do not get changed on a frequent basis.

Application servers will provide more complex and dynamic service logic that can potentially make use of additional information not available directly via SIP messages (e.g. location, time, day etc.).

The IMS Service profile is defined and maintained in the HSS and its scope is limited to IM CN Subsystem. The service profile is downloaded from the HSS to the S-CSCF. Only one service profile per Public user identity is downloaded to the S-CSCF at a given time (such as at registration, update of a profile etc.) based on the Public user identities being served by the S-CSCF. Nothing precludes that multiple service profiles can be defined in the HSS for a subscription. Each Public user identity is associated with one and only one Service Profile. Each service profile is associated with one or more Public user identities.

An ISIM application shall securely store the home domain name of the subscriber. It shall not be possible for the UE to modify the information from which the home domain name is derived.

It is not a requirement for a user to be able to register on behalf of another user which is third party registration specified in [12] or for a device to be able to register on behalf of another device or for combinations of the above for the IM CN subsystem for this release.

Public User Identities may be shared across multiple UEs. Hence, a particular Public User Identity may be simultaneously registered from multiple UEs that use different Private User Identities and different contact addresses. Subscription data may restrict a user from having the same Public User Identity simultaneously registered from multiple contact addresses. ~~–~~If a Public User Identity belongs to an IMS subscription and it is shared among the Private User Identities, then it is assumed that all Private User Identities in the IMS subscription share the Public User Identity ~~within the IMS subscription~~. The relationship for such a shared Public User Identity with Private User Identities, and the resulting relationship with service profiles and IMS subscription, is depicted in Figure 4.6 ~~below~~. An IMS subscription may support multiple IMS users.

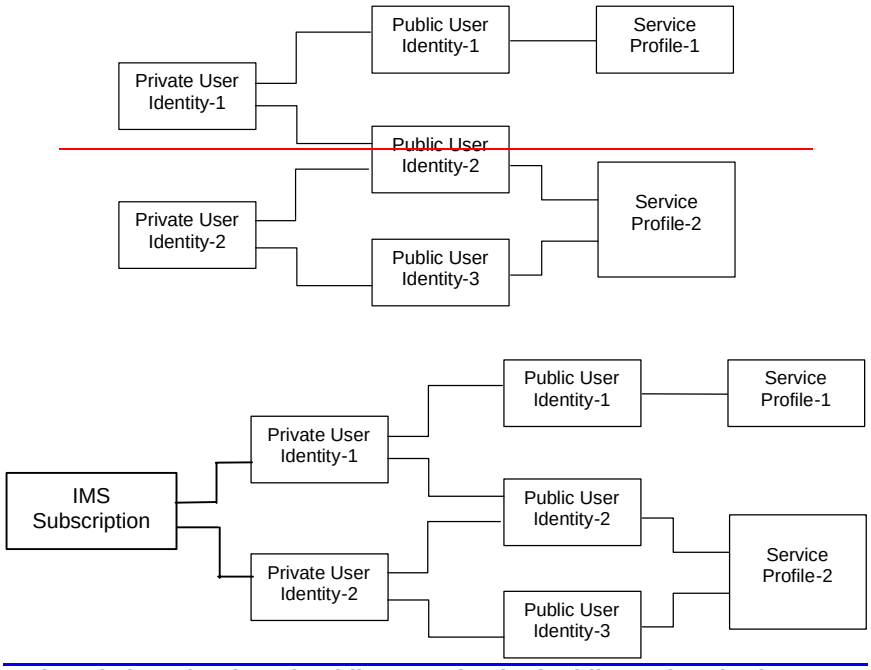


Figure 4.6 – The relation of a shared Public User Identity (Public-ID-2) and Private User Identities

All Service Profiles of a user, which share at least one common Private user identity through their relationship to public user identities, shall be associated to the same S-CSCF. Later releases may allow different Service Profiles that share the same Private user identity to be associated with different S-CSCFs.

All Service Profiles of a user shall be stored in the same HSS, even if the user has one or more shared Public User identities.

4.3.4 Identification of network nodes

The CSCF, BGCF and MGCF nodes shall be identifiable using a valid SIP URL (Host Domain Name or Network Address) on those interfaces supporting the SIP protocol, (e.g. Gm, Mw, Mm, and Mg). These SIP URLs would be used when identifying these nodes in header fields of SIP messages. However this does not require that these URLs will be globally published in DNS.

***** Next Change *****

4.7 Multimedia Resource Function

The architecture concerning the Multimedia Resource Function is presented in Figure 4.5a below.

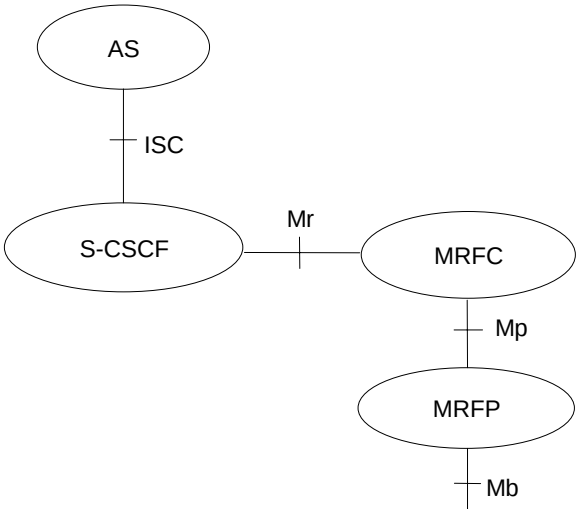


Figure 4.~~5a~~7: Architecture of MRF

The MRF is split into Multimedia Resource Function Controller (MRFC) and Multimedia Resource Function Processor (MRFP).

Tasks of the MRFC are the following:

- Control the media stream resources in the MRFP.
- Interpret information coming from an AS and S-CSCF (e.g session identifier) and control MRFP accordingly.
- Generate of CDRs.

Tasks of the MRFP are the following:

- Control of the bearer on the Mb reference point.
- Provide resources to be controlled by the MRFC.
- Mixing of incoming media streams (e.g for multiple parties).
- Media stream source (for multimedia announcements).
- Media stream processing (e.g. audio transcoding, media analysis).

Tasks of an Application Server with regards to MRF are e.g. the following:

- Conference booking and provide booking information (e.g. start time, duration, list of participants) to the MRFC.
- Provide a floor control mechanism, by which end users (e.g. participants, chairman) can influence floor and provide information to the MRFC on how incoming media streams should be mixed and distributed accordingly.

The protocol used for the Mr reference point is SIP (as defined by RFC 3261 [12], other relevant RFC's, and additional enhancements introduced to support 3GPP´s needs).

The Mp reference point allows an MRFC to control media stream resources provided by an MRF.

The Mp reference point has the following properties:

- Full compliance with the H.248 standard.
- Open architecture where extensions (packages) definition work on the interface may be carried out.

The protocol for the Mp reference point is not specified in this release.

***** Next Change *****

5.2.1a Implicit Registration

When an user has a set of public user identities defined to be implicitly registered via single IMS registration of one of the public user identity's in that set, it is considered to be an Implicit Registration. No single public identity shall be considered as a master to the other public user identities. Figure 5.~~2.1a~~0b shows a simple diagram of implicit registration and public user identities. Figure 5.0c shows a similar diagram when multiple private user identities are involved. In order to support this function, it is required that:

- HSS has the set of public user identities that are part of implicit registration.
- Cx reference point between S-CSCF and HSS shall support download of all public user identities associated with the implicit registration, during registration of any of the single public user identities within the set.
- All public user identities of an Implicit Registration set must be associated to the same private user identities. See figure 5.2.1.b for the detailed relationship between the public and private user entities within an Implicit Registration set.
- When one of the public user identities within the set is registered, all Public user identities associated with the implicit registration set are registered at the same time.
- When one of the public user identities within the set is de-registered, all public user identities that have been implicitly registered are de-registered at the same time.
- Registration and de-registration always relates to a particular contact address. A Public user identitity that has been registered (including when implicitly registered) with different contact addresses remains registered in relation to those contact addreses that have not been de-registered.
- Public user identities belonging to an implicit registration set may point to different service profiles; or some of these public user identities may point to the same service profile.
- When a public user identity belongs to an implicit registration set, it cannot be registered or de-registered individually without the public user identity being removed from the implicit registration list.
- All IMS related registration timers should apply to the set of implicitly registered public user identities
- S-CSCF, P-CSCF and UE shall be notified of the set of public user identities belonging to the implicitly registered function. Session set up shall not be allowed for the implicitly registered public user identities until the entities are updated, except for the explicitly registered public user identity.
- The S-CSCF shall store during registration all the Service profiles corresponding to the public user identities being registered.
- When a public user identity is barred from IMS communications, only the HSS and S-CSCF shall have access to this public user identity.

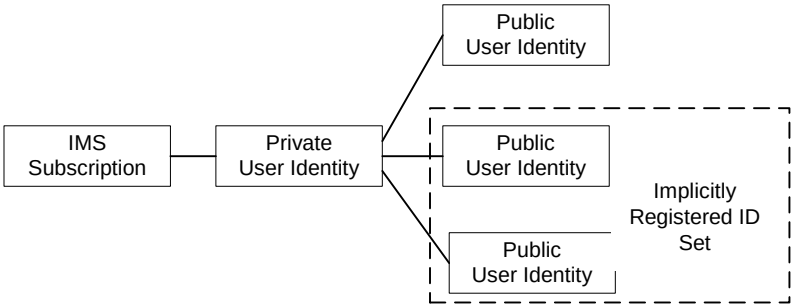


Figure 5.~~2.1a~~0b Relationship of public user identities when implicitly registered

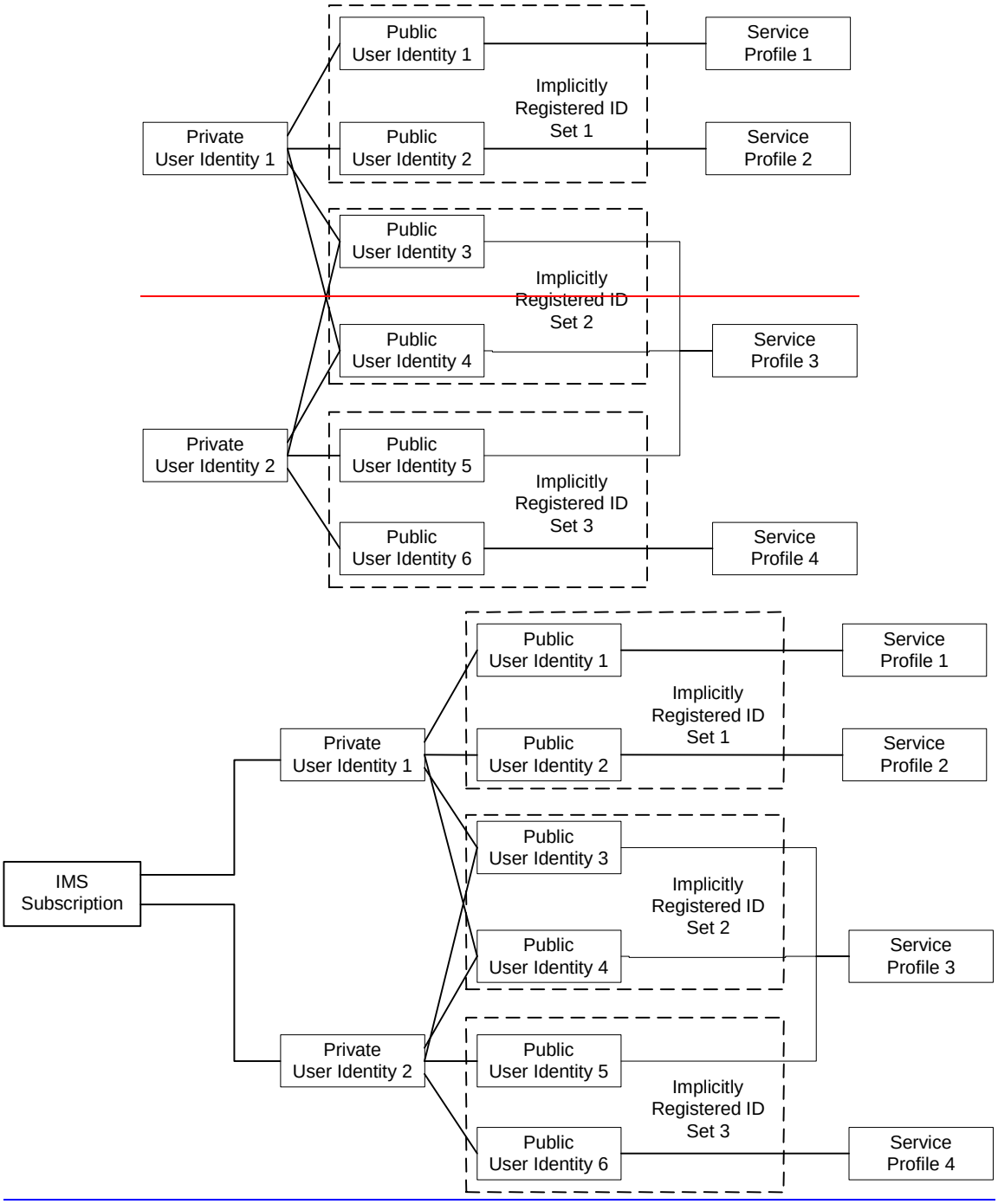


Figure 5.~~2.1.b~~0c – The relation of two shared Public User Identities (Public-ID-3 and 4) and Private User Identities

5.2.1a.1 Implicit Registration for UE without ISIM

In case an UE is registering in the IMS without ISIM, it shall require the network's assistance to register atleast one public user identity, which is used for session establishment & IMS signalling. Implicit registration shall be used as part of a mandatory function for these ISIM-less UEs to register the public user identity(s). In addition to the functions defined in section 5.2.1a, the following additional functions are required for this scenario.

- The Temporary public identity shall be used for initial registration process
- It shall be defined in HSS that if the user does not have implicit registration activated then the user shall not be allowed to register in the IMS using the Temporary public user identity.

Tdoc S2-040952

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **405** ⌘ **rev** **1** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Resource reservation in IMS
Source:	⌘	SA2 (Nokia)
Work item code:	⌘	IMS2
Date:	⌘	16/02/2004
Category:	⌘	**C**
Release:	⌘	Rel-6

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

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

Reason for change: ⌘ During the course of developping IMS architectural support for session-based messaging it became apparent that the existing resource reservation and QoS-assured pre-conditions mechanism is unnecessarily complex for messaging sessions. The messaging media component does not require QoS beyond best effort, hence it is expected that there will be no need to reserve additional bearer resources, but already established resources (PDP Context) can be used.

By introducing this procedure for IMS messaging sessions, the UE as well as the network need to provide certain means for using already established IP-CAN bearers. This behaviour is thought to be beneficial also for other services where no additional resource reservation is required.

In fact, using pre-established bearer resources should be a general capability for IMS from Rel-6 onwards. This ensures that the network resources are used in an optimal manner conforming to the needs of the particular service being applied.

Summary of change: ⌘ The relevant sections of the specification are enhanced to allow for using pre-established bearer resources.

Consequences if not approved: ⌘

Clauses affected: ⌘ 4.2.5, 5.4.8

Other specs affected: ⌘

Y	N	
	X	Other core specifications
	X	Test specifications
	X	O&M Specifications

⌘

Other comments: ⌘

How to create CRs using this form:

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

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

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

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

********** First change **********

4.2.5 The QoS requirements for an IM CN subsystem session

The selection, deployment, initiation and termination of QoS signalling and resource allocation shall consider the following requirements so as to guarantee the QoS requirement associated with an IM CN subsystem session.

1. Independence between QoS signalling and Session Control

   The selection of QoS signalling and resource allocation schemes should be independent of the selected session control protocols. This allows for independent evolution of QoS control and the session control in the IM CN subsystem.

2. Necessity for End-to-End QoS Signalling and Resource -Allocation

   End-to-end QoS indication, negotiation and resource allocation during the session set-up in the IM CN subsystem should be enforced for those services and applications that require QoS better than best-effort.

4. Restricted Resource Access at the IP BS Level

   Access to the resources and provisioning of QoS at IP BS Level should be authenticated and authorised by applying appropriate QoS policies via the IP Policy Control element

5. Restricted Resource Access at the IP-Connectivity Access Network (i.e. layer-2) Level

   Access to the resources and provisioning of QoS at the IP-Connectivity Access Network Level should be authenticated and authorised by using existing registration/security/QoS policy control mechanisms of the IP-CAN.

6. Co-ordination between Session Control and QoS Signalling/Resource Allocation

   a. In establishing an IMS session, it shall be possible for an application to request that the resources needed for bearer establishment be successfully allocated before the destination user is alerted.

   b. In establishing an IMS session, it shall be possible, dependent on the application being offered, to prevent the use of the bearer until the session establishment is completed.

   c. In establishing an IMS session, it shall be possible for a terminating application to allow the destination user to participate in determining which bearers shall be established.

   d. Successful bearer establishment shall include the completion of any required end-to-end QoS signalling, negotiation and resource allocation.

   e. In establishing an IMS session, it shall be possible to use already allocated bearer resources, if these resources fulfill the needs of the session. However, note that QoS policy control mechanisms of the IP-CAN may not allow to use already allocated bearer resources.

   The initiation of any required end-to-end QoS signalling, negotiation and resource allocation processes at different network segments shall take place after the initiation and delivery of a session set-up request.

7. The Efficiency of QoS Signalling and Resource Allocation

   The sequence of end-to-end QoS signalling, negotiation and resource allocation processes at different network segments should primarily consider the delay in negotiating end-to-end QoS and reserving resources that contributes to the session set-up delay. Parallel or overlapping QoS negotiation and resource reservation shall be allowed where possible.

8. Dynamic QoS Negotiation and Resource Allocation

   Changes (upgrading or downgrading) of QoS provided to an active IMS session shall be supported based on either the request from the IM application or the current network loads or link quality (e.g. radio link quality).

   It shall be possible to maintain a resource allocation in excess of the resources needed for current media flows (but within the restrictions imposed by points #4 and #5 above), in order to e.g. switch to different media flow characteristics without risk of admission control failure.

9 Prevention of Theft of Service

The possibility for theft of service in the IM CN subsystem shall be no higher than that for the corresponding packet data and circuit switched services.

10 Prevention of Denial of Service

The system unavailability due to denial of service attacks in the IM CN subsystem shall be no greater than that for the corresponding packet data and circuit switched services.

********** Second change **********

5.4.8 QoS-Assured Preconditions

This section contains concepts for the relation between the resource reservation procedure and the procedure for end-to-end sessions.
A precondition –is a set of constraints about the session, which are introduced during the session initiation. The recipient of the session generates an answer, but does not alert the user or otherwise proceed with session establishment until the preconditions are met. This can be known through a local event (such as a confirmation of a resource reservation), or through a new set of constraints sent by the caller.

A "QoS-Assured" session will not complete until required resources have been allocated to the session. In a QoS-Assured session, the UE must succeed in establishing the QoS bearer for the media stream according to the QoS preconditions defined at the session level before it may indicate a successful response to complete the session and alert the other end point. The principles for when a UE shall regard QoS preconditions to be met are:

- A minimum requirement to meet the QoS preconditions defined for a media stream in a certain direction, is that an appropriate IP-CAN bearer established at the local access for that direction.

- Segmented resource reservation is performed since the end points are responsible to make access network resource reservations via local mechanisms.

- The end points shall offer the resources it may want to support for the session and negotiate to an agreed set. Multiple negotiation steps may be needed in order to agree on a set of media for the session. –The final agreed set is then updated between the end points.

- The action to take in case a UE fails to fulfil the pre-conditions (e.g. failure in establishment of an RSVP session) depends on the reason for failure. If the reason is lack of resources in the network (e.g. an admission control function in the network rejects the request for resources), the UE shall fail to complete the session. For other reasons (e.g. lack of RSVP host or proxy along the path) the action to take is local decision within the UE. It may for example 1) choose to fail to complete the session, 2) attempt to complete the session by no longer requiring some of the additional actions.

The following cases exist in the context of using "QoS-Assured" preconditions for IMS:

a. The IMS session requires the reservation of additional bearer resources, and the UE requires confirmation from the other endpoint of the fulfilment of the pre-conditions related to this resource reservation. Alternatively, the UE may not require explicit confirmation from the other SIP endpoint when the pre-conditions are fulfilled. One example of such SIP endpoint is the MGCF used for PSTN interworking. In these cases, one or both of the reservation confirmation messages may not be sent.

b. The IMS session does not require the reservation of additional bearer resources, and both endpoints indicate in their initial session setup message that the pre-conditions are fulfilled.

c. The IMS session does not require the reservation of additional bearer resources, and the endpoints do not use the mechanism to indicate "QoS-Assured" pre-conditions.

Note: The flows of sections 5.5, 5.6 and 5.7 depict the case where both UEs require confirmation from eachother of the fulfilment of the pre-conditions.

~~The flows of sections 5.5, 5.6 and 5.7 depict the case where both UEs require confirmation from the other of the fulfilment of the pre-conditions. Other cases are possible according to the SIP specifications. For example, the pre-~~

~~conditions may already be fulfilled (according to the principles above) when the INVITE is sent, or the UE may not require explicit confirmation from the other SIP endpoint when the pre-conditions are fulfilled. One example of such SIP endpoint is the MGCF used for PSTN interworking. In these cases, one or both of the reservation confirmation messages may not be sent.~~

********** End of changes **********

3GPP TSG-SA2 Meeting #38
Atlanta, USA, 16 – 20 February 2004

Tdoc ⌘S2-040953

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **406** ⌘**rev** **1** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Architectural support for AS origination
Source:	⌘	SA2 (Nokia)
Work item code:	⌘	IMS2
Date:	⌘	16/02/2004
Category:	⌘	**C**
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The current stage-2 specification defines the requirement for Application Servers to originate requests on behalf of users. However, the detailed architectural support for this capability is yet to be defined. To provide full flexibility to services over IMS, the capability of allowing ASs to originate requests on behalf of users should be adequately specified.
Summary of change:	⌘	Text has been added introducing the support in the S-CSCF for Application Server generated originating SIP requests and dialogs on behalf of users and PSIs. A new flow has been introduced for AS origination. The de-registration section has been modified to indicate the need for keeping the S-CSCF name in the HSS in case unregistered services apply.
Consequences if not approved:	⌘	

Clauses affected:	⌘	4.6.3, 5.3.1, 5.3.2.1, new section 5.6.5

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

Other comments:	⌘	

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

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

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

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

First modified section

4.6.3 Serving-CSCF

The Serving-CSCF (S-CSCF) performs the session control services for the UE. It maintains a session state as needed by the network operator for support of the services. Within an operator's network, different S-CSCFs may have different functionalities. The functions performed by the S-CSCF during a session are:

Registration

- May behave as a Registrar as defined in RFC 3261 [12] or subsequent versions, i.e. it accepts registration requests and makes its information available through the location server (eg. HSS).

Session-related and session-unrelated flows

- Session control for the registered endpoint's sessions. It shall reject IMS communication to/from public user identity(s) that are barred for IMS communications after completion of registration, as described in subclause 5.2.1.
- May behave as a Proxy Server as defined in RFC 3261 [12] or subsequent versions, i.e. it accepts requests and services them internally or forwards them on, possibly after translation.
- May behave as a User Agent as defined in RFC 3261 [12] or subsequent versions, i.e. it may terminate and independently generate SIP transactions.
- Interaction with Services Platforms for the support of Services
- Provide endpoints with service event related information (e.g. notification of tones/announcement together with location of additional media resources, billing notification)
- ~~On behalf of~~For an originating endpoint (i.e. the originating user/UE, or originating AS)
  - Obtain from a database the Address of the I-CSCF for the network operator serving the destination user from the destination name (e.g. dialled phone number or SIP URL), when the destination user is a customer of a different network operator, and forward the SIP request or response to that I-CSCF.
  - When the destination name of the destination user (e.g. dialled phone number or SIP URL), and the originating user is a customer of the same network operator, forward the SIP request or response to an I-CSCF within the operator's network.
  - Depending on operator policy, forward the SIP request or response to another SIP server located within an ISP domain outside of the IM CN subsystem.
  - Forward the SIP request or response to a BGCF for call routing to the PSTN or CS Domain.
  - In case the request is an originating request from an Application Server:
    - Verify that the request coming from the AS is an originating request, and apply procedures accordingly (e.g. invoke interaction with Service Platforms for originating services, etc…);
    - Process and proceed with the request even if the user on whose behalf the AS had generated the request is unregistered.
    - Process and proceed with other requests to and from the user on whose behalf the AS had generated the request.
    - Reflect in the charging information that an AS has initiated the session on behalf of a user.
- ~~On behalf of~~For a destination endpoint (i.e. the terminating user/UE)
  - Forward the SIP request or response to a P-CSCF for a MT procedure to a home user within the home network, or for a user roaming within a visited network where the home network operator has chosen not to have an I-CSCF in the path

- Forward the SIP request or response to an I-CSCF for a MT procedure for a roaming user within a visited network where the home network operator has chosen to have an I-CSCF in the path.
- Modify the SIP request for routing an incoming session to CS domain according to HSS and service control interactions, in case the user is to receive the incoming session via the CS domain.
- Forward the SIP request or response to a BGCF for call routing to the PSTN or the CS domain.

Charging and resource utilisation:

- Generation of CDRs

Next modified sections

5.3 Application level de-registration procedures

5.3.1 Mobile initiated de-registration

When the UE wants to de-register from the IMS then the UE shall perform application level de-registration. De-registration is accomplished by a registration with an expiration time of zero seconds. De-registration follows the same path as defined in subclause 5.2.2.3 “Registration Information Flow – User not registered”.

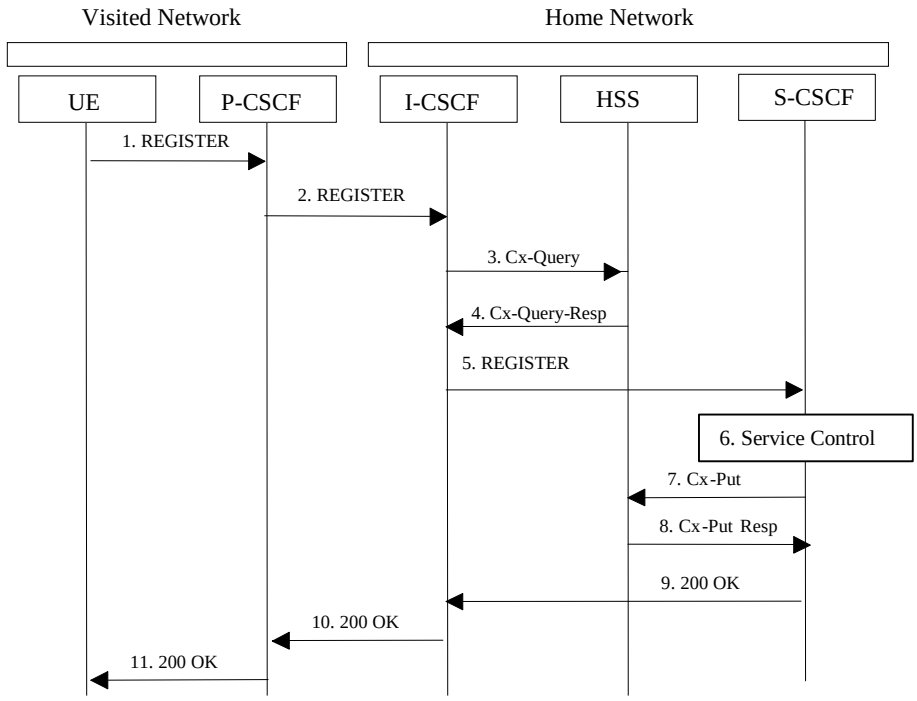


Figure 5.3: De-registration - user currently registered

1. The UE decides to initiate de-registration. To de-register, the UE sends a new REGISTER request with an expiration value of zero seconds. The UE sends the REGISTER information flow to the proxy (public user identity, private user identity, home network domain name, UE IP address).
2. Upon receipt of the register information flow, it shall examine the “home domain name” to discover the entry point to the home network (i.e. the I-CSCF). The proxy does not use the entry point cached from prior registrations. The proxy shall send the Register information flow to the I-CSCF (P-CSCF address/name, public user identity, private user identity, P-CSCF network identifier, UE IP address). A name-address resolution mechanism is utilised in order to determine the address of the home network from the home domain name. The P-CSCF network identifier is a string that identifies at the home network, the network where the P-CSCF is located (e.g., the P-CSCF network identifier may be the domain name of the P-CSCF network).

3. The I-CSCF shall send the Cx-Query information flow to the HSS (public user identity, private user identity, P-CSCF network identifier).

4. The HSS shall determine that the public user identityuser is currently registered. The Cx-Query Resp (indication of entry point, e.g. S-CSCF) is sent from the HSS to the I-CSCF.

5. The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism and then shall send the de-register information flow (P-CSCF addres/name, public user identity, private user identity, UE IP address, I-CSCF(THIG) in case network configuration hiding is desired) to the S-CSCF.

6. Based on the filter criteria, the S-CSCF shall send de-registration information to the service control platform and perform whatever service control procedures are appropriate. Service control platform removes all subscription information related to this specific public user identity.

7. Based on operator choice the S-CSCF can send either Cx-Put (public user identity, private user identity, clear S-CSCF name) or Cx-Put (public user identity, private user identity, keep S-CSCF name), and the public user identity is no longer considered registered in the S-CSCF. In case the user has (originating – see 5.6.5, or terminating – see 5.12) services related to unregistered state, the S-CSCF sends Cx-Put (public user identity, private user identity, keep S-CSCF name) in order to keep the S-CSCF name in the HSS for these services.

   The HSS then either clears or keeps the S-CSCF name for that public user identity according to the Cx-Put request. In both cases the state of the public user identity is stored as unregistered in the HSS. If the S-CSCF name is kept, then the HSS shall be able to clear the serving S-CSCF name at any time.

8. The HSS shall send Cx-Put Resp to the S-CSCF to acknowledge the sending of Cx-Put.

9. The S-CSCF shall return the 200 OK information flow to the I-CSCF. The S-CSCF may release all registration information regarding this specific registration of the public user identity after sending information flow 200 OK.

10. The I-CSCF shall send information flow 200 OK to the P-CSCF.

11. The P-CSCF shall send information flow 200 OK to the UE. The P-CSCF releases all registration information regarding this specific registration of the public user identity after sending information flow 200 OK.

5.3.2 Network initiated de-registration

If an ungraceful session termination occurs (e.g. flat battery or mobile leaves coverage), when a stateful proxy server (such as the S-CSCF) is involved in a session, memory leaks and eventually server failure can occur due to hanging state machines. To ensure stable S-CSCF operation and carrier grade service, a mechanism to handle the ungraceful session termination issue is required. This mechanism should be at the SIP protocol level in order to guarantee access independence for the IM CN subsystem.

The IM CN subsystem can initiate a Network Initiated De-Registration procedures for the following reasons:

- Network Maintenance.
  Forced re-registrations from users, e.g. in case of data inconsistency at node failure, in case of UICC lost, etc. Cancelling the current contexts of the user spread among the IM CN Subsystem network nodes at registration, and imposing a new IM registration solves this condition.

- Network/traffic determined.
  The IM CN subsystem must support a mechanism to avoid duplicate registrations or inconsistent information storage. This case will occur when a user roams to a different network without de-registering the previous one. This case may occur at the change of the roaming agreement parameters between two operators, imposing new service conditions to roamers.

- Application Layer determined.
  The service capability offered by the IM CN Subsystem to the Application Layers may have parameters specifying whether all IM CN subsystem registrations are to be removed, or only those from one or a group of terminals from the user, etc.

- Subscription Management
  The operator must be able to restrict user access to the IM CN subsystem upon detection of contract

expiration, removal of IM subscription, fraud detection, etc.In case of changes in service profile of the user, e.g. the user subscribes to new services, it may possible that new S-CSCF capabilities, which are required from the S-CSCF, are not supported by the current S-CSCF which has been assigned to the user. In this case, it shall be possible to actively change the S-CSCF by using the network initiated de-registration by HSS procedure.

The following sections provide scenarios showing SIP application de-registration. Note that these flows have avoided the strict use of specific SIP protocol message names. This is in an attempt to focus on the architectural aspects rather than the protocol.

Two types of network-initiated de-registration procedures are required:

- To deal with registrations expirations.
- To allow the network to force de-registrations following any of the approved possible causes for this to occur.

5.3.2.1 Network Initiated Application (SIP) De-registration, Registration Timeout

The following flow shows a network initiated IM CN subsystem terminal application (SIP) de-registration based on a registration timeout. A timer value is provided at initial registration and is refreshed by subsequent re-registrations. The flow assumes that the timer has expired. The locations (home or visited network) of the P-CSCF and S-CSCF are not indicated as the scenario remains the same for all cases.

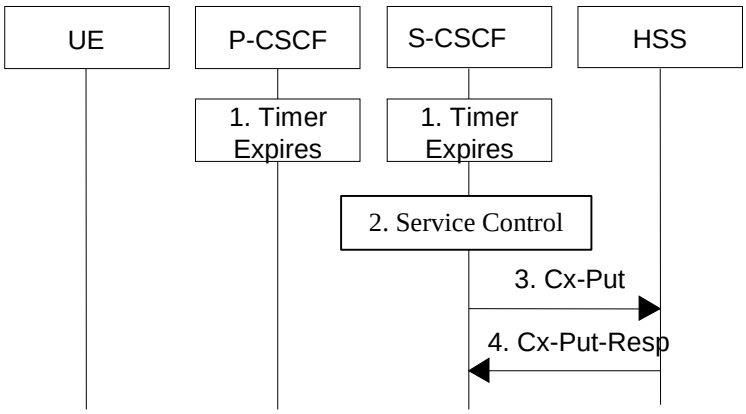


Figure 5.4: Network initiated application de-registration, registration timeout

1. The registration timers in the P-CSCF and in the S-CSCF expire. The timers are assumed to be close enough that no external synchronisation is required. The P-CSCF updates its internal databases to remove the public user identity from being registered. It is assumed that any cleanup of IP-Connectivity Access Network resources will be handled by independent means.

2. Based on the filter criteria, the S-CSCF shall send de-registration information to the service control platform and perform whatever service control procedures are appropriate. Service control platform removes all subscription information related to this specific public user identity.

3. Based on operator choice the S-CSCF can send either Cx-Put (public user identity, private user identity, clear S-CSCF name) or Cx-Put (public user identity, private user identity, keep S-CSCF name), and the public user identity is no longer considered registered in the S-CSCF. In case the user has (originating – see 5.6.5, or terminating – see 5.12) services related to unregistered state, the S-CSCF sends Cx-Put (public user identity, private user identity, keep S-CSCF name) in order to keep the S-CSCF name in the HSS for these services.

   The HSS then either clears or keeps S-CSCF name for that public user identity according to the Cx-Put request. In both cases the state of the public user identity is stored as unregistered in the HSS. If the S-CSCF name is kept, then the HSS shall be able to clear the serving S-CSCF name at any time.

4. The HSS shall send Cx-Put Resp to the S-CSCF to acknowledge the sending of Cx-Put.

5.3.2.2 Network Initiated Application (SIP) De-registration, Administrative

For different reasons (e.g., subscription termination, lost terminal, etc.) a home network administrative function may determine a need to clear a user's SIP registration. This function initiates the de-registration procedure and may reside in various elements depending on the exact reason for initiating the de-registration.

One such home network element is the HSS, which already knows the S-CSCF serving the user and that for this purpose makes use of the Cx-Deregister. Another home network element that could initiate the de-registration is the S-CSCF, in which case it makes use of the Cx-Put to inform the HSS. Other trusted/secured parties may also initiate de-registration to the S-CSCF.

The following flow shows a network initiated IM CN subsystem terminal application (SIP) de-registration based on an administrative action for example. The IP transport infrastructure is not notified. If complete packet access is to be denied, a transport layer administrative mechanism would be used. This scenario does not address the administrative mechanisms used for updating any subscriber records, EIR records, access authorisation, etc. This scenario only addresses the specific action of clearing the SIP application registration that is currently in effect.

As determined by the operator, on-going sessions may be released by using network initiated session release procedures in Section 5.10.3.

Added new section

5.6.5 Application Server origination

This origination procedure applies to an Application Server that intiates a session on behalf of a user (i.e. a Public User Identity) or a Public Service Identity. In case the AS initiates the session on behalf of a user, the identity-related fields of the initial request are populated the same way as if the request was originated by the user himself.

In case of originating unregistered procedures, the handling of the S-CSCF in the HSS will follow the same principle as terminating unregistered user handling.

The procedure described below assumes that the Application Server takes care of the user plane connection.

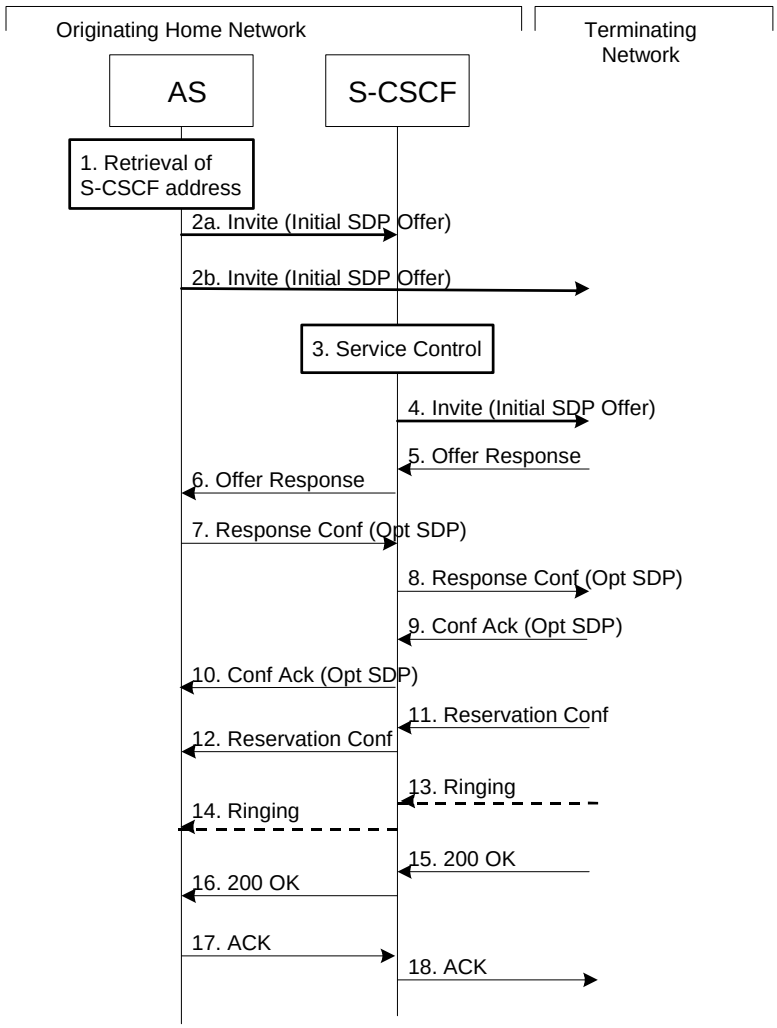


Figure 5.16d: Application Server origination procedure

Procedure for Application Server origination is as follows:

1. The Application Server acquires the address of the S-CSCF (if not available already) for the Public User Identity or the Public Service Identity on whose behalf the AS intends to originate the session. The AS may then proceed in the following way:

   - If the AS could not acquire a S-CSCF address for the Public User Identity, the AS shall not initiate a session on behalf of the user.

   - If the Public Service Identity on whose behalf the AS intends to generate the session does not have a S-CSCF address allocated, the AS sends the session initiation request directly towards the terminating network. In this case the AS may use the principles defined in RFC 3263 “Session Initiation Protocol (SIP): Locating SIP Servers” (see step 2b) to route the session initiation request.

   - If the AS has acquired a S-CSCF address for the Public Service Identity or the Public User Identity, the AS sends the session initiation request to the S-CSCF (see step 2a).

2a. The AS sends the SIP INVITE request, containing an initial SDP, to the S-CSCF.
The initial SDP may represent one or more media for a multi-media session.

2b. The AS sends the SIP INVITE request, containing an initial SDP, to the terminating network.

The subsequent steps assume that the session initiation procedure involves the S-CSCF, i.e.they show the continuation of step 2a.

3. S-CSCF identifies the incoming request as an originating request, and invokes any origination service logic required for this Public User Identity / Public Service Identity. The S-CSCF handles the incoming request as an authenticated and authorized request, as it was originated by a trusted entity within the network.

4. S-CSCF forwards the request, as specified by the S-S procedures.

5-6. The media stream capabilities of the destination are returned along the signalling path.

7-8. The AS decides the offered set of media streams for this session, confirms receipt of the Offer Response and sends the Response Confirmation along the signaling path towards the destination network. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response or a subset. The AS is free to continue to offer new media on this operation or on subsequent exchanges using the Update method.

9-10. The terminating end point responds to the originating end with an acknowledgement, which is forwarded along the session signaling path. If Optional SDP is contained in the Response Confirmation, the Confirmation Acknowledge will also contain an SDP response.

11-12. The terminating endpoint responds to the originating end when successful resource reservation has occured.

13-14. The destination UE may optionally perform alerting. If so, it signals this to the originating party by a provisional response indicating Ringing. This message is sent to the AS along the signaling path.

15-16. When the destination party answers, the terminating endpoint sends a SIP 200-OK final response along the signalling path to the originating end.

17-18. The AS responds to the 200 OK with an ACK message which is passed along the signalling path to the terminating end.

End of modifications

3GPP TSG-SA2 Meeting #38
Atlanta, USA, 16 – 20 February 2004

Tdoc ⌘S2-041021

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **407** ⌘ **rev** **2** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Clarification of forking capabilities
Source:	⌘	SA2 (Nokia)
Work item code:	⌘	IMS2
Date:	⌘	16/02/2004
Category:	⌘	**C**
Release:	⌘	Rel-6

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

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

Reason for change:	⌘	The current specification allows the UE to indicate its capabilities upon registration. The purpose of indicating these capabilities is to provide information to the S-CSCF whether and how the incoming session initiation requests are to be forked across the contact addresses. However, this purpose is currently not described. Additionally, the current specification states that the AS may act as a forking proxy in the sense of RFC 3261. By definition, this would require the AS to acquire knowledge about the registered contact addresses. This is not possible with IMS registration-related procedures, there is no mechanism for the S-CSCF to pass the registered contact address information of the UE to the AS.
Summary of change:	⌘	The description of the forking functionality has been amended to describe forking based on UE-indicated capabilities. The description of the AS-forking has been amended to clarify that the IM CN Subsystem does not provide mechanisms for the Application Server to receive the contact address(es) of the UE upon IMS registration. Instead, the AS can e.g. use Presence-based mechanisms to acquire the contact addresses. Also, the capability for the AS to "fork" across Public IDs has been removed from the Sections describing forking, as it is not this behaviour of the AS is not forking in the sense of RFC 3261.
Consequences if not approved:	⌘	

Clauses affected:	⌘	4.2.7.2

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

How to create CRs using this form:

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

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

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

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

First modified section

4.2.7 Support of SIP forking

4.2.7.1 SIP Forking

SIP forking is the ability of a SIP proxy server to fork SIP request messages to multiple destinations according to RFC 3261 [12].

4.2.7.2 Forking within and outside the IM CN Subsystem

The IM CN subsystem shall have the capability to fork requests to multiple destinations; this capability is subject to rules for forking proxies defined in RFC 3261 [12].

- The S-CSCF shall support the ability for a public user identity to be registered from multiple contact addresses, as defined in RFC 3261 [12]. The S-CSCF shall support forking so that an incoming SIP request addressed to a Public User Identity is proxied to multiple registered contact addresses. This allows forking across multiple contact addresses of the same Public User Identity.

- When multiple contact addresses have been registered, then the S-CSCF shall exhibit the following behaviour with regards to forking the incoming SIP request:~~.~~

    1. If the UE has indicated capability information upon IMS registration in terms of SIP User Agent capabilities and characteristics described in “draft-ietf-sip-callee-caps-01” [38], then the S-CSCF shall use it to generate a target contact set using the matching mechanism described in "draft-ietf-sip-callerprefs-10" [xx]. If the UE has not indicated any capabilities for the contact addresses upon registration, then the S-CSCF may still use the preference information, if indicated for the contact addresses upon registration, as described in the following bulletpoint below.

    2. If the UE has indicated preference information for contact addresses upon registration, then the S-CSCF shall use it to decide if parallel or sequential forking is used across the contact addresses that have matching callee capabilities, as described in RFC 3261 [12]. If the UE has not indicated any preference for the matching contact addresses upon registration, or if the preferences for the matching contact addresses have equal value, then it is up to the configuration of the S-CSCF if parallel or sequential forking is to be performed across the contact addresses that have matching callee capabilities.

- Application Servers in the IMS may act as a forking proxy in the sense of RFC 3261 [12].

    Note: The AS may subscribe to the registration event package to retrieve the contact address(es) of the UE.

- ~~and may fork a SIP request across multiple Public User Identities allocated to the same user.~~ S-CSCFs shall provide the necessary support for forking by Application Servers.

Additionally, other networks outside the IM CN Subsystem are able to perform SIP forking.

4.2.7.3 Support for forked requests

UE and MGCF shall be ready to receive responses generated due to a forked request and behave according to the procedures specified in [12] and in this section.

The UE and MGCF may accept or reject early dialogues from different terminations as described in [12], for example if the UE is only capable of supporting a limited number of simultaneous dialogs.

Upon the reception of a first final 200 OK (for INVITE), the UE or MGCF shall acknowledge the 200 OK and cancel other early dialogues that may have been established. In this case the UE or MGCF may require updating the allocated resources according to the resources needed. In case it receives a subsequent 200 OK, the UE or MGCF shall acknowledge the dialogue and immediately send a BYE to drop the dialog.

The UE and MGCF may include preferences, in INVITE's, indicating that proxies should not fork the INVITE request.

On the terminating side, UE and MGCF shall be able to receive, as specified in [12], several requests for the same dialog that were forked by a previous SIP entity.

Application Servers and MRFCs shall be capable to handle forked requests according to the procedures specified in [12].

End of modified sections

3GPP TSG-SA WG2 Meeting #38
Atalanta, USA, 16-20 February 2004

Tdoc ⌘S2-040969

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **408** ⌘ **rev** **1** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	PSIs for local services
Source:	⌘	SA2 (Siemens)
Work item code:	⌘	IMS-2
Date:	⌘	18/02/2004
Category:	⌘	**F**
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	With the introduction of PSIs there are standardized means for addressing and routing local services. However the existing text goes back to the Release-5 time frame and therefore does not use the PSI terminology.
Summary of change:	⌘	Introduce statement that a local service may be identified by a globally routable PSI. Add PSI terminology in the existing text. Clarify how the VPLMN is recognised.
Consequences if not approved:	⌘	Relationship between PSIs and local services remains undefined and may trigger misunderstandings, e.g. in stage 3 design.

Clauses affected:	⌘	4.2.2

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

Other comments:	⌘	

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

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be

downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

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

4.2.2 Support of Local Services in the IMS

Visited network provided services offer an opportunity for revenue generation by allowing access to services of a local nature to visiting users (inbound roamers). There shall be a standardised means to access local services. The mechanism to access local services shall be ~~exactly~~ the same for home users and inbound roamers.

A local service may be identified by a globally routable public service identity (PSI); see subclause 4.3.6 for the definition of a PSI. In this case the routing principles in subclause 5.4.12 apply.

However, in some cases it is necessary to identify a local service by an identifier, which is not globally routable, e.g. using a local addressing plan. In this case ~~A~~access to local services shall be provided in the following manner:

1. It shall be possible for the HPLMN to determine whether the roaming user is requesting a local service, or is "dialing" an address according to the local addressing plan. This shall be based upon an indication received from the UE. The same indication shall be used to access local services as well as to use the local addressing plan. This indication shall be included in the Request URI of the SIP Invite.

2. The P-CSCF shall route the session towards the S-CSCF as per the session origination procedures.

3. Processing the SIP URI (e.g. address analysis and potential modification such as translation into globally routable format, e.g. a globally routable PSI) shall be performed by an Application Server in the subscriber's Home Network. The S-CSCF routes the session towards this Home Network Application Server based upon filter criteria which are triggered by the 'local indication' received from the UE. If required, the AS may need to identify the VPLMN, e.g. from information in SIP signalling or via the Sh interface.

4. The AS passes the session request back to the S-CSCF and~~T~~ the S-CSCF routes the session, via normal ~~SIP~~ IMS routing principles, towards its destination (e.g. a server in the VPLMN identified by a PSI). Note that ~~T~~the ISC interface is not used as an inter-operator interface.

There shall be a standardised mechanism for the UE that is registered in the IM Subsystem, to receive and/or retrieve information about the available local services. It shall be possible to advertise local services to a registered UE independent of whether the UE has an active SIP session. Local services may be presented e.g. by directing the user to a web page.

Note: For users who have roamed, services relevant to the locality of the user may also be provided by the home network.

3GPP TSG-SA WG2 Meeting #38
Atlanta, USA, 16-20 February 2004

Tdoc ⌘S2-041022

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** **409** ⌘ **rev** **2** ⌘ Current version: **6.4.1** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Group management clarification
Source:	⌘	SA2 (Siemens)
Work item code:	⌘	IMS-2
Date:	⌘	19/02/2004
Category:	⌘	C
Release:	⌘	Rel-6

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	IMS groups are managed via the Ut reference point. Stage 1 requires "the IMS group management shall provide the ability for users to create groups that can be utilized in context of different services." The current stage 2 description leaves it unclear whether there is the possibilty to share groups between applications on a common group and list management server or whether they need to be configured on each application server seperately.
Summary of change:	⌘	Clarify that the Ut reference point shall support a scenario where one single Application Server is used to create groups that can be utilized for different services.
Consequences if not approved:	⌘	Stage 1 requirement not fulfilled.

Clauses affected:	⌘	3.3, 4.10.1

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

Other comments:	⌘	

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

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

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

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

*** FIRST CHANGE ***

3.3 Abbreviations

For the purposes of the present document the following abbreviations apply. Additional applicable abbreviations can be found in GSM 01.04 [1].

AMR	Adaptive Multi-rate
API	Application Program Interface
AS	Application Server
BCSM	Basic Call State Model
BG	Border Gateway
BGCF	Breakout Gateway Control Function
BS	Bearer Service
CAMEL	Customised Application Mobile Enhanced Logic
CAP	Camel Application Part
CDR	Charging DataRecord
CN	Core Network
CS	Circuit Switched
CSCF	Call Session Control Function
CSE	CAMEL Service Environment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ENUM	E.164 Number
GGSN	Gateway GPRS Support Node
GLMS	Group and List Management Server
GMLC	Gateway Mobile Location Centre
GUP	Generic User Profile
HSS	Home Subscriber Server
I-CSCF	Interrogating-CSCF
IETF	Internet Engineering Task Force
IM	IP Multimedia
IM CN SS	IP Multimedia Core Network Subsystem
IMS	IP Multimedia Core Network Subsystem
IMS ALG	IMS Application Level Gateway
IMSI	International Mobile Subscriber Identifier
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IP-CAN	IP-Connectivity Access Network
ISDN	Integrated Services Digital Network
ISIM	IMS SIM
ISP	Internet Service Provider
ISUP	ISDN User Part
MAP	Mobile Application Part
MGCF	Media Gateway Control Function
MGF	Media Gateway Function
NAI	Network Access Identifier
NA(P)T-PT	Network Address (Port-Multiplexing) Translation-Protocol Translation
OSA	Open Services Architecture
P-CSCF	Proxy-CSCF
PDF	Policy Decision Function
PDN	Packet Data Network
PDP	Packet Data Protocol e.g., IP
PEF	Policy Enforcement Function
PLMN	Public Land Mobile Network
PSI	Public Service Identity
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RAB	Radio Access Bearer

RFC	Request for Comments
SCS	Service Capability Server
S-CSCF	Serving-CSCF
SGSN	Serving GPRS Support Node
SLF	Subscription Locator Function
SSF	Service Switching Function
SS7	Signalling System 7
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SGW	Signalling Gateway
THIG	Topology Hiding Inter-network Gateway
TrGW	Translation Gateway
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
URL	Universal Resource Locator
USIM	UMTS SIM

*** NEXT CHANGE ***

4.10 IMS group management concepts

This clause describes architectural concepts to fulfil the requirements for IMS Group Management described in TS 22.250 [32].

4.10.1 IMS group administration

The capabilities required for IMS group management are defined in clause 5.4 of TS 22.250 [32]. The Ut reference point is used to manage groups from the UE. This does not preclude the use of other mechanisms for group management, e.g. using OSA or OA&M mechanisms; the details of these other mechanisms are out of scope of this document.

The Ut reference point shall support a scenario where one single Application Server is used to create groups that can be utilized for different services, possibly hosted by different ASes.

Note: Such an Application Server is sometimes referred to as a Group and List Management Server (GLMS).

4.10.2 Group identifiers

Each group shall be addressable by a globally unique group identifier. The group identifier shall take the form of a Public Service Identifier.

3GPP TSG-SA WG2 Meeting #38
Atlanta, USA, 16-20 February 2004

Tdoc ⌘S2-040828

CR-Form-v7

CHANGE REQUEST

⌘ **23.228** **CR** 410 ⌘**rev** **-** ⌘ Current version: **5.11.0** ⌘

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

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Relation of IMS sessions and PDP Contexts
Source:	⌘	SA2 (Ericsson)
Work item code:	⌘	IMS-CCR
Date:	⌘	06/02/2004
Category:	⌘	**F**
Release:	⌘	Rel-5

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

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	During the course of Rel5 development some mechanisms were introduced to allow the IMS network to control the groupping of media components to PDP Contexts. These mechanisms were put in place to ensure that appropriate charging can be performed with the underlying charging capabilities of Rel5 GPRS networks. As this mechanism only apply in case of SBLP, CN1 has had the understanding that the SA2-CN3 correspondance on this topic only has been for cases involving SBLP. Without SBLP and charging correlation, any reason to prevent re-use of a PDP context between multiple SIP sessions cannot be seen (except in case the network has indicated this by the 'keep it separate' indicator). Alignment with rel-6 and stage 3.
Summary of change:	⌘	Clarifying that when SBLP and KIS is applied then media components from different sessions can not use same IP bearers, but if such restrictions don't apply then UE may choose to use same bearers for different sessions.
Consequences if not approved:	⌘	Misalignment between CN1 and SA2 specs

Clauses affected:	⌘	4.2.5.1

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

Other comments:	⌘	

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

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

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

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

*** FIRST AND ONLY CHANGE ***

4.2.5.1 Relation of IMS media components and PDP contexts carrying IMS media

The relation between IMS media components and PDP contexts carrying IMS media may be~~is~~ controlled by the IMS network on media component level in the following way:

The P-CSCF ~~shall have the capability to~~ indicates to the UE that a separate PDP Context is required for each IMS media component indicated. The P-CSCF shall apply and maintain the same policy to separate specific media components into separate PDP Contexts during a session. If a media component is added during the session, the new decision on the separation for the media components shall not contradict any former decisions. For mobile originating sessions the P-CSCF shall apply the policy to the initial offer to ensure identical decisions for different answers, e.g. a media component not required to use a separate PDP Context initially, shall not later require a separate PDP Context (e.g. in case of subsequent answers received due to forking).

- If the UE receives such an indication for a media component, it shall open a separate PDP Context for this media component. If the UE receives no such indication for a media component, the UE makes the decision whether to open a separate PDP Context or modify an existing PDP Context for this media component.

- The criteria and information for setting this indication is determined by local policy in the network where the P-CSCF is located.

Note: the bearer charging capabilities of the P-CSCF's network, and the capabilities of deployed UEs should be taken into account when defining such policies in the visited IMS network operator's domain.

- The IMS network shall have the capability to transfer the media component level indication described above to the UE. It shall be possible to~~This media component level indication shall be~~ transfer~~red~~ this media component level information in SIP/SDP signaling upon session initiation and addition of media component(s) to active IMS sessions.

When service based local policy is used, i~~I~~t is assumed that media components from different IMS sessions are not carried within the same PDP context. When service based local policy is not used, the UE may decide to carry media components from different IMS sessions within the same PDP context (without contradicting any previous and new requirement that media components are to be handled separately), as the network does not police how the UE groups media components to PDP contexts.

All associated IP flows (such as e.g. RTP / RTCP flows) used by the UE to support a single media component are assumed to be carried within the same PDP context.