Source: **TSG SA WG2**

Title: **CR(s) to 23.228**

Agenda item: **7.2.3**

Document for: **APPROVAL**

S2 Tdoc	Title	Spec	CR	Rev	Cat	C_Ver	Rel	WI
S2-050525	Corrections to the Network initiated Application de-registration	23.228	473	3	F	6.8.0	Rel-6	IMS2
S2-050424	Correction to the Refer operation	23.228	474	2	F	6.8.0	Rel-6	IMS2
S2-050389	Editorial corrections in the identity procedures	23.228	475	1	F	6.8.0	Rel-6	IMS2
S2-050280	Corrections for errors introduced in 23.228 reorganization	23.228	478		F	6.8.0	Rel-6	IMS2
S2-050339	Corrections to flow for codec change	23.228	479	1	F	6.8.0	Rel-6	IMS2
S2-050335	Update of reference to TEL URI RFC 3966	23.228	481	1	F	6.8.0	Rel-6	IMS2
S2-050340	SBLP interactions correction	23.228	482	1	F	6.8.0	Rel-6	QoS1

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **23.228 CR 473** | ⌘ **rev 3** ⌘ | Current version: | **6.8.0** | ⌘ |

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: ⌘	Corrections to the Network initiated Application de-registration			
Source: ⌘	3GPP TSG_SA WG2			
Work item code:⌘	IMS2		**Date:** ⌘	17/01/2005
Category: ⌘	**F**		**Release:** ⌘	Rel-6

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

Use <u>one</u> of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change: ⌘	Some text in section 5.3.2.2.2 is redundant as they are already described in section 5.3.2.2.0. And in section 5.3.2.2.2 the step 6 and 7 describe that the S-CSCF sends an update to the HSS to remove itself as the registered S-CSCF for this user. But the S-CSCF may save other services related to unregistered state for this public user identity. In this case the S-CSCF shall have opportunity to indicate the HSS that its name shall be kept.
Summary of change: ⌘	1. Delete the redundant text in section 5.3.2.2.2 2. Add an indication to the Cx-Put in step 6 to indicate whether the S-CSCF name shall be cleared in the HSS or not
Consequences if not approved: ⌘	There is redundant text in this section and the S-CSCF have no opportunity to determine whether its name shall be cleared in the HSS or not.

Clauses affected: ⌘	5.3.2.2.2

	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.

<div style="border:2px solid black; text-align:center;">

**** First modified section ****

</div>

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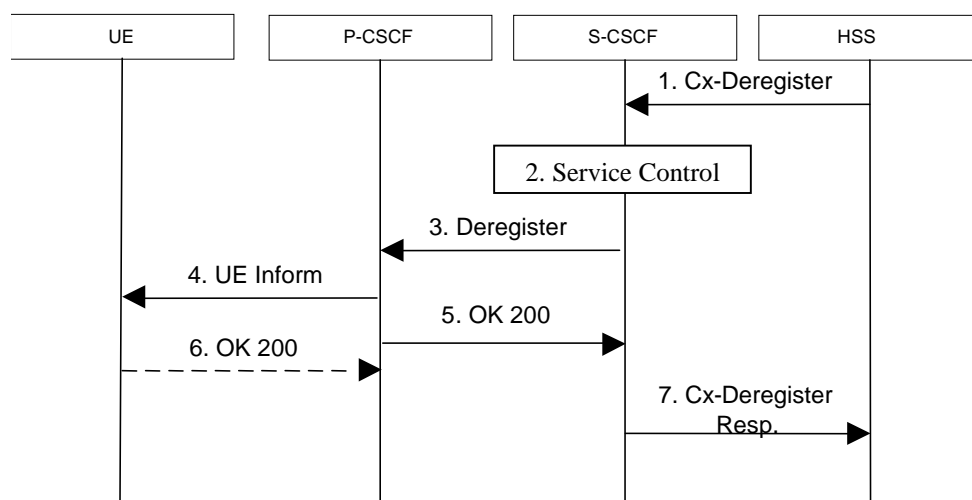
Figure 5.5: Network initiated application de-registration by HSS, administrative

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 Service Platform~~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.~~
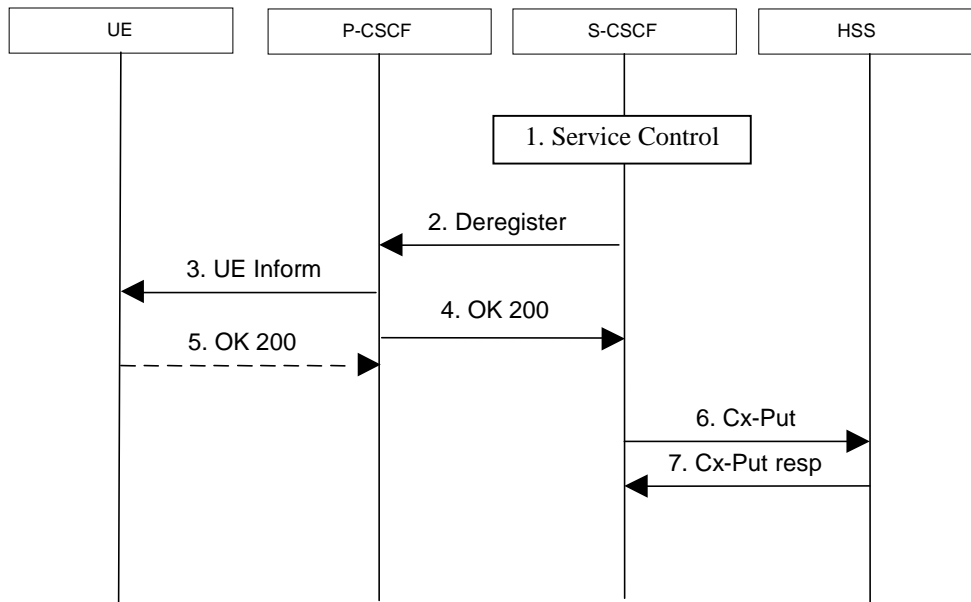
Figure 5.5a: Network initiated application de-registration, service platform

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.~~

6. 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). In both cases 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 may send 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 Cx-Put the request. In both cases the state of the Public User Identity stored in the HSS indicates that the Public User Identity is unregistered in the S-CSCF.

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

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.

<< End of changed clause >>

CR-Form-v7.1

CHANGE REQUEST

⌘	**23.228** CR **474**	⌘**rev** **2** ⌘	Current version:	**6.8.0** ⌘

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

Title: ⌘	Correction to the Refer operation	
Source: ⌘	3GPP TSG_SA WG2	
Work item code:⌘	IMS2	***Date:*** ⌘ 17/01/2005
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:
  Ph2 *(GSM Phase 2)*
  R96 *(Release 1996)*
  R97 *(Release 1997)*
  R98 *(Release 1998)*
  R99 *(Release 1999)*
  Rel-4 *(Release 4)*
  Rel-5 *(Release 5)*
  Rel-6 *(Release 6)*
  Rel-7 *(Release 7)*

Reason for change: ⌘	In the figure 5.42 the UE#1 issues the BYE message to clear the session with UE#2.In the following section 5.11.6.2 the original session is always cleared by the Initiator of the Refer Operation, that is UE#2. To be consistent I propose that the last BYE message in the figure 5.42 is issued by the UE#2, although the last BYE message can be sent either by the UE#1 or by the UE#2,
Summary of change:⌘	The last BYE message in the figure 5.42 is issued by UE#2.
Consequences if not approved: ⌘	Inconsistency between the section 5.11.6.2 and the section 5.11.6.1.

Clauses affected: ⌘	5.11.6.1

	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.
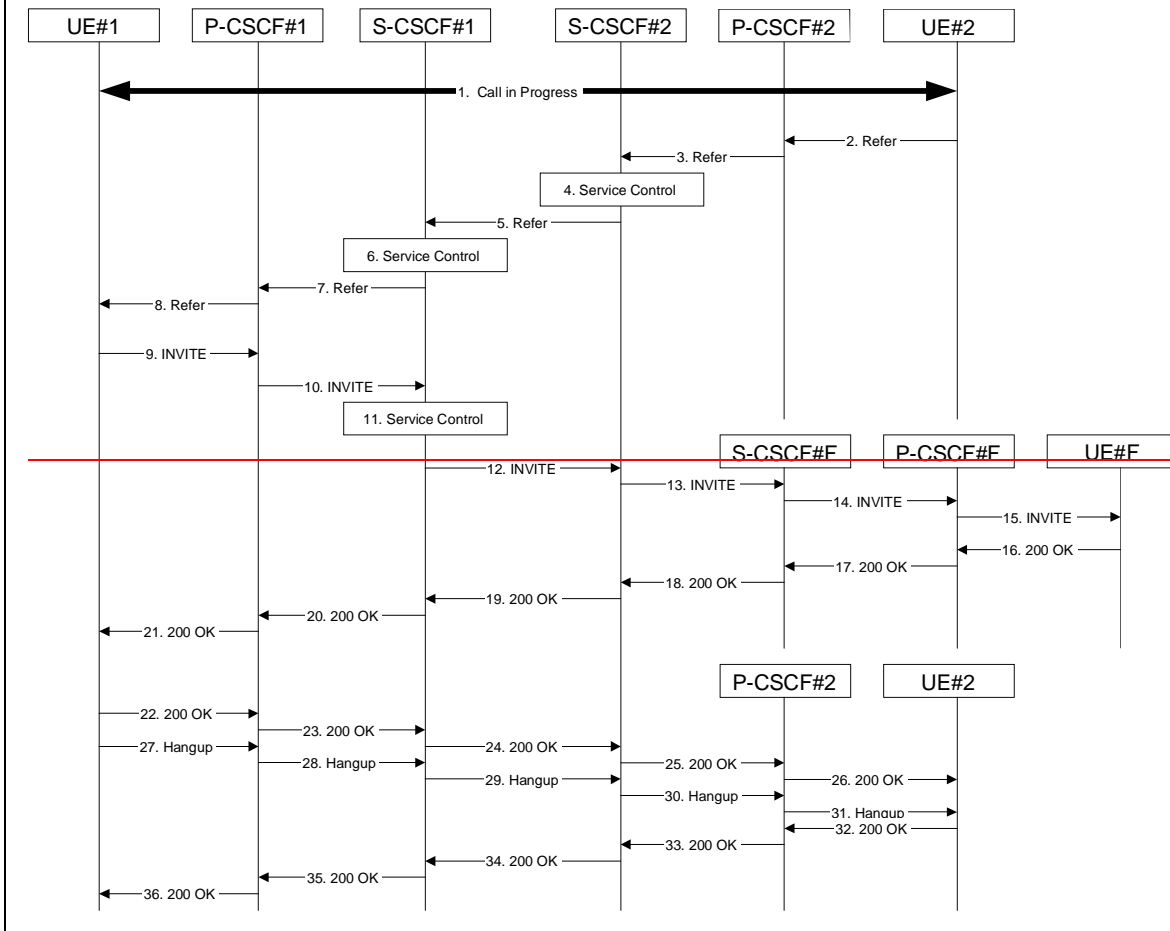
> ****** First modified section ******

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". The end point receiving a referral may be UE#1 as shown in the example flow in figure 5.42 or it may be any other type of originating entity as defined in subclause 5.4.10. The referring endpoint may be either UE#2 as shown, an Application Server or a non-IMS network SIP client. The referred-to destination may be UE#F as shown in figure 5.42 or it may be any other type of terminating entity as defined in subclause 5.4.10. Only the scenario in which a call from the first UE is referred by a second UE to a third UE is shown.

An information flow illustrating this is as follows:

| UE#1 | P-CSCF#1 | S-CSCF#1 | S-CSCF#2 | P-CSCF#2 | UE#2 |

1. Call in Progress
2. Refer
3. Refer
4. Service Control
5. Refer
6. Service Control
7. Refer
8. Refer
9. INVITE
10. INVITE
11. Service Control

| S-CSCF#F | P-CSCF#F | UE#F |

12. INVITE
13. INVITE
14. INVITE
15. INVITE
16. 200 OK
17. 200 OK
18. 200 OK
19. 200 OK
20. 200 OK
21. 200 OK

| P-CSCF#2 | UE#2 |

22. 200 OK
23. 200 OK
24. 200 OK
25. 200 OK
26. 200 OK
27. Hangup
28. Hangup
29. Hangup
30. Hangup
31. Hangup
32. 200 OK
33. 200 OK
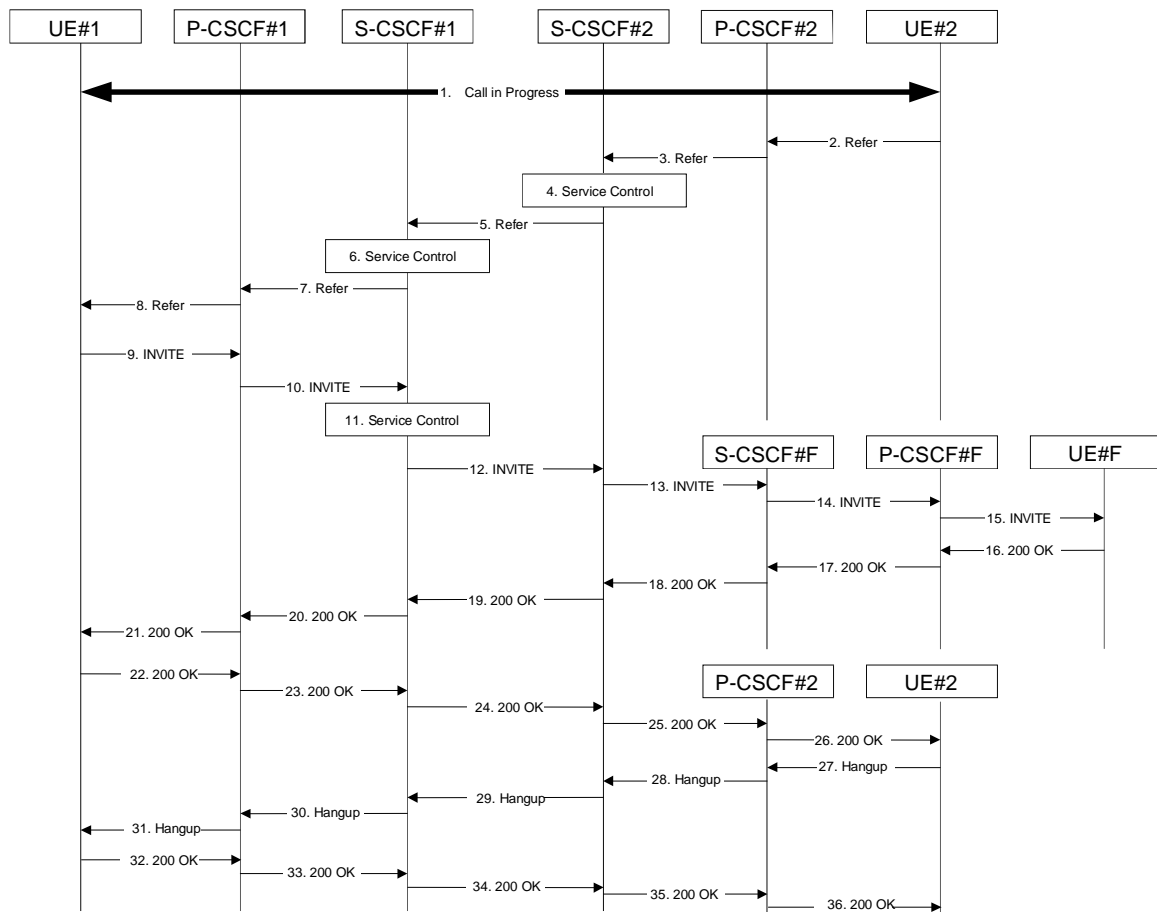34. 200 OK
35. 200 OK
36. 200 OK

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 subclause.

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 URI, addressed to itself, with the new destination information and the billing information that will be needed for the new session. It replaces the "Refer-To" value in the request with the private URI.

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 URIs, 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 URI 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 URI, 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 URI destination, and determines the final destination of the new session. It determines the network operator addressed by the destination URI. 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#2 clears the original session with UE#1 by sending the BYE message. This message is routed through P-CSCF#2, S-CSCF#2, S-CSCF#1, P-CSCF#1, to UE#1.

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

Note: The last BYE message to clear the original session can be issued either by UE#1 or by 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.

<< End of changed clause >>

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **23.228 CR 475** | ⌘**rev 1** | ⌘ | Current version: | **6.8.0** | ⌘ |

*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:	⌘	Editorial corrections in the identity procedures	
Source:	⌘	3GPP TSG_SA WG2	
Work item code:⌘	IMS2	*Date:* ⌘	17/01/2005
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:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change:	⌘	The figure 5.35 in section 5.11.4.2 is incorrectly missing a service control box in S-CSCF#2.
Summary of change:⌘		Add the missing service control box in the figure and add some clarifications in the section 5.11.4.2
Consequences if not approved:	⌘	Inconsistency between the figure and the text

Clauses affected:	⌘	5.11.4.2		

		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 ****

5.11.4.2   Procedures for blocking the identity of the originating party

Regulatory agencies, as well as subscribers, may require the ability of an originating party to block the display of their identity either permanently or on a session by session basis. This is a function performed by the destination P-CSCF. In this way, the terminating party is still able to do a session-return, session-trace, transfer, or any other supplementary service.

In this call flow, it is assumed that privacy has been required by UE#1 on Public User Identity (i.e. 'id' privacy) .
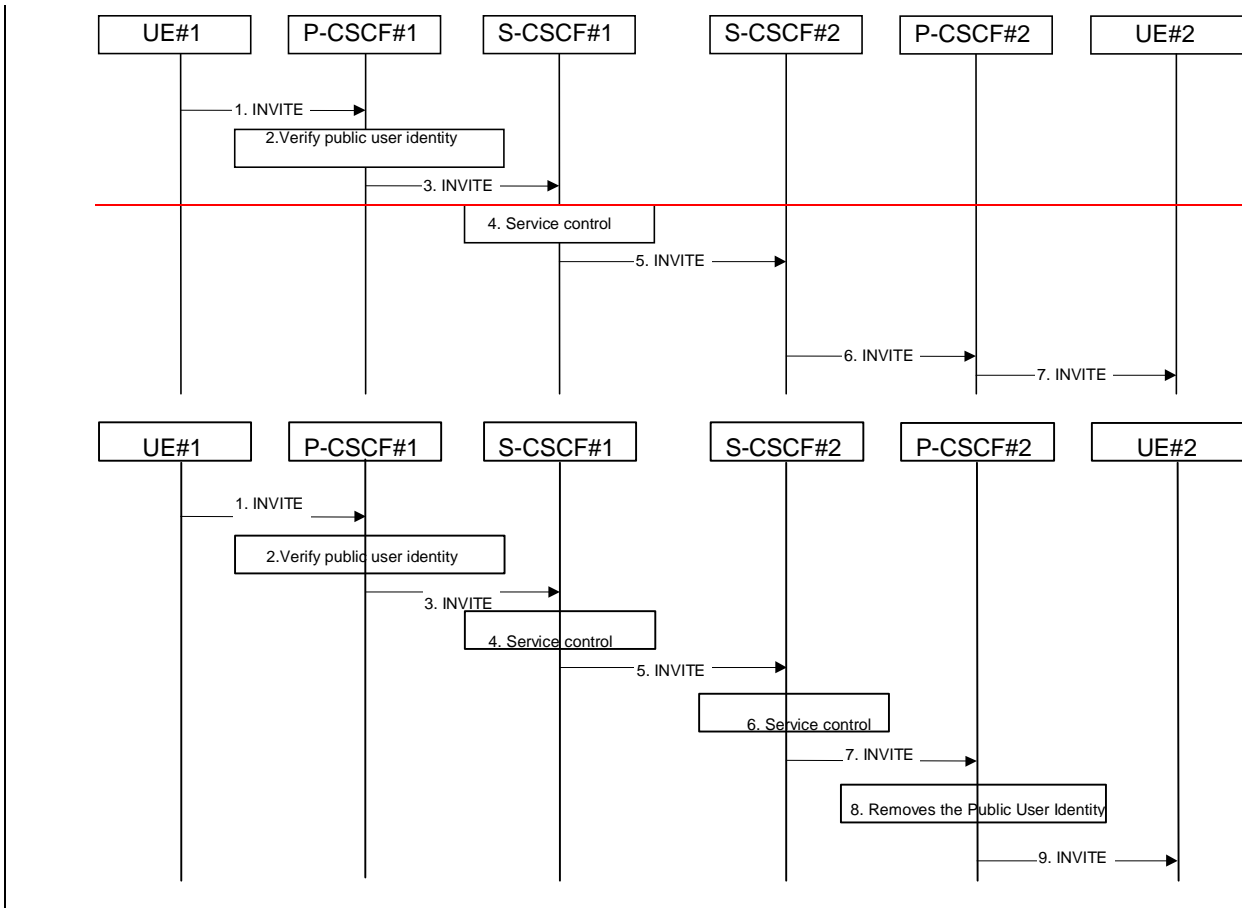
Figure 5.35: Blocking the identity of the originating party

The detailed procedure is as follows:

1. UE#1 initiates a new multi-media session, by sending an INVITE request to P-CSCF#1. This INVITE request includes Public User Identity, and may include a display name that may identify the specific person using the UE. Also included in this INVITE message is an indication that the identity of the originating party shall not be revealed to the destination.

2. P-CSCF#1 checks the Public User Identity of the originating party, and replaces it (or rejects the request) if it is incorrect.

3. P-CSCF#1 forwards the INVITE request, with the verified Public User Identity , to S-CSCF#1.

4. S-CSCF#1 invokes whatever service logic is appropriate for this session set up attempt. Based on the subscriber's profile, S-CSCF#1 may insert an indication in the INVITE message that the identity of the originating party shall not be revealed to the terminating party. S-CSCF#1 may insert an indication to block the IP address of UE#1 too and may remove other information from the messaging which may identify the caller to the terminating party.

5. S-CSCF#1 forwards the INVITE request, with verified Public User Identity, and with user-name of the originating party if present, to S-CSCF#2.

6. If the terminating party has an override functionality in S-CSCF#2/Application Server in the terminating network the S-CSCF#2/Application Server removes the indication of privacy from the message.

7. S-CSCF#2 forwards the INVITE request to P-CSCF#2.

8. If privacy of the user identity is required, P-CSCF#2 removes the Public User Identity from the message.

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

<< End of changed clause >>

CR-Form-v7

CHANGE REQUEST

⌘	**23.228** CR	**478**	⌘**rev**	**-**	⌘	Current version:	**6.8.0**	⌘	

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: ⌘	Corrections for errors introduced in 23.228 reorganization	
Source: ⌘	3GPP TSG_SA WG2	
Work item code:⌘	IMS2	***Date:*** ⌘ 26/01/2005
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)
Rel-7 (Release 7)

Reason for change: ⌘	TS 23.228 was recently re-organized to make the new R6 material fit better with the organization of the document. During this reorganization some errors were introduced.
Summary of change:⌘	Some duplicate rows of table 5.2 are removed and a number of incorrectly formatted figure numbers are corrected. In addition a duplicate figure number is corrected.
Consequences if not approved: ⌘	Potential implementation errors due to misunderstanding the document.

Clauses affected: ⌘	4.2.3, 4.7, 5.4a, 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.6.4, 5.6.5, 5.7.4, 5.7a, and 5.8.4

		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 *****

4.2.3   Support of roaming users

The architecture shall be based on the principle that the service control for Home subscribed services for a roaming subscriber is in the Home network, e.g., the Serving-CSCF is located in the Home network.
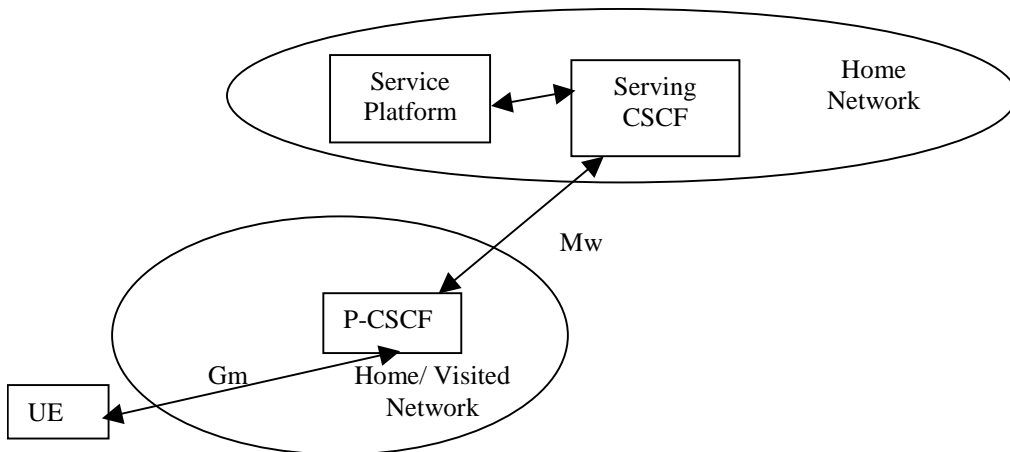
Figure 4-14.1: Service Platform in Home Network
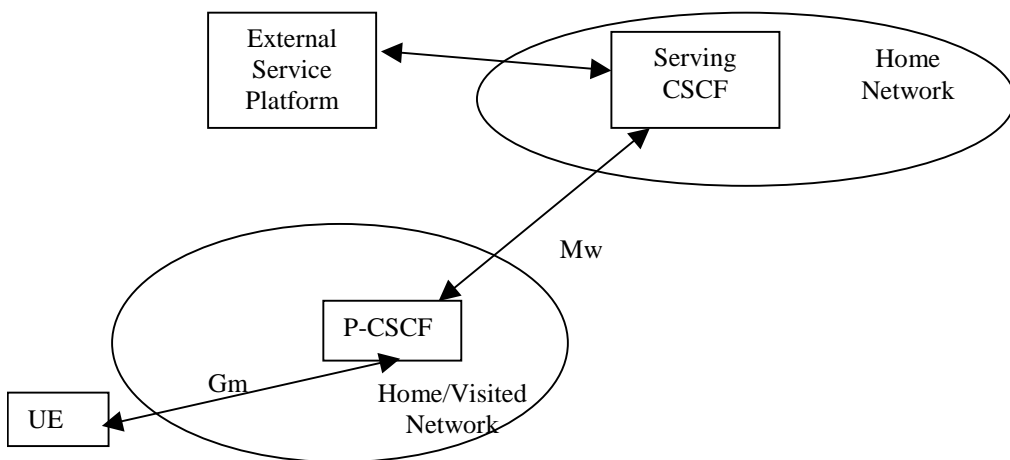
Figure 4-24.2: External Service Platform

There are two possible scenarios to provide services:

- via the service platform in the Home Network

- via an external service platform (e.g. third party or visited network)

The external service platform entity could be located in either the visited network or in the 3rd party platform. The standardised way for secure 3rd party access to IMS services is via the OSA framework, see section 4.2.4.

The roles that the CSCF plays are described below.

- The Proxy-CSCF shall enable the session control to be passed to the Serving-CSCF.

- The Serving-CSCF is located in the home network. The Serving-CSCF shall invoke service logic.

A Proxy-CSCF shall be supported in both roaming and non-roaming case, even when the Serving-CSCF is located in the same IM CN Subsystem.

Reassigning the Proxy-CSCF assigned during CSCF discovery is not a requirement in this release. Procedures to allow registration time Proxy-CSCF reassignment may be considered in future releases.

Procedures shall be supported to allow assigning different Proxy-CSCFs when a user registers from multiple UE(s) simultaneously.

Network initiated Proxy-CSCF reassignment is not a requirement.

The use of additional CSCFs, that is Interrogating-CSCF (THIG)s, to be included in the SIP signalling path is optional. Such additional CSCFs may be used to shield the internal structure of a network from other networks. See also sub-clauses 4.4 and 4.6.2.1.

***** Next Change *****

4.7   Multimedia Resource Function

The architecture concerning the Multimedia Resource Function is presented in Figure 4.5a 4.7 below.
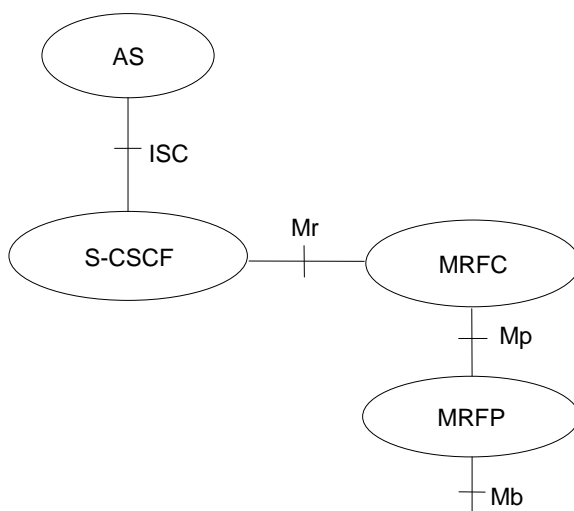
Figure 4.7: Architecture of MRF

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 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).

- Floor Control (i.e. manage access rights to shared resources in a conferencing environment).

Tasks of an Application Server with regards to MRF are e.g. the following:

- Conference booking and management of booking information (e.g. start time, duration, list of participants)

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.

***** Next Change *****

5.4a   Overview of session flow procedures

This section contains the overview description and list of individual procedures for the end-to-end session flows.

For an IP Multi-Media Subsystem session, the session flow procedures are shown in the following diagram.
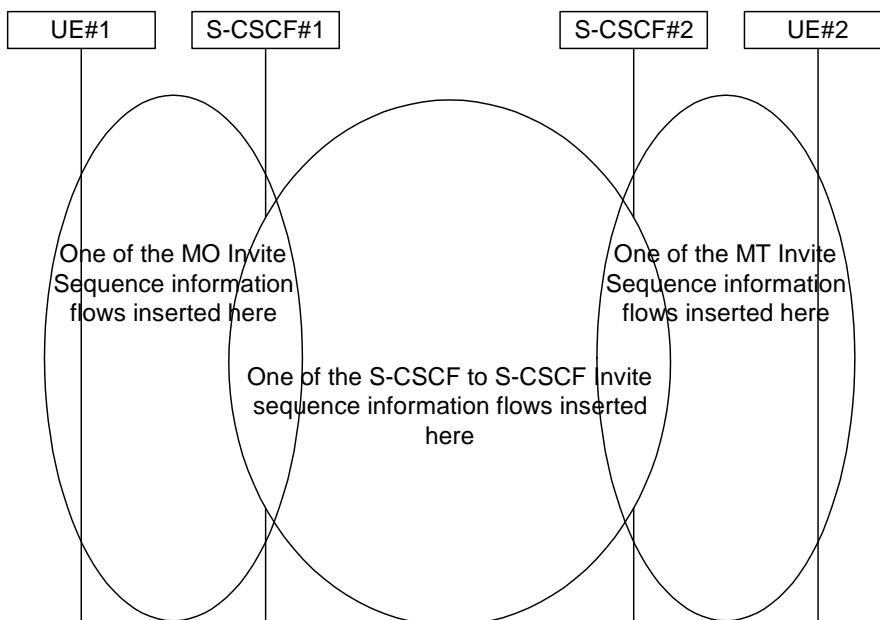
Figure 5.9: Overview of Session Flow Sections

The following procedures are defined:

For the origination sequences:

- (MO#1) Mobile origination, roaming , see subclause 5.6.1

- (MO#2) Mobile origination, home, see subclause 5.6.2

- (PSTN-O) PSTN origination, see subclause 5.6.3

- (NI-O) Non-IMS network origination (external SIP client), see subclause 5.6.4

- (AS-O) Application Server origination, see subclause 5.6.5

For the termination sequences:

- (MT#1) Mobile termination, roaming, see subclause 5.7.1

- (MT#2) Mobile termination, home, see subclause 5.7.2

- (MT#3) Mobile termination, CS Domain roaming, see subclause 5.7.2a

- (PSTN-T) PSTN termination, see subclause 5.7.3

- (NI-T) Non-IMS network termination (external SIP client), see subclause 5.7.4

- (AS-T#1) PSI based Application Server termination, direct, see subclause 5.7.5

- (AS-T#2) PSI based Application Server termination, indirect, see subclause 5.7.6

- (AS-T#3) PSI based Application Server termination, direct, using DNS, see subclause 5.7.7

- (AS-T#4) PUI based Application Server termination, indirect, see subclause 5.7.8

For Serving-CSCF/MGCF-to-Serving-CSCF/MGCF sequences:

- (S-S#1) Session origination and termination are served by different network operators, see subclause 5.5.1

- (S-S#2) Session origination and termination are served by the same operator, see subclause 5.5.2

- (S-S#3) Session origination with PSTN termination in the same network as the S-CSCF, see subclause 5.5.3

- (S-S#4) Session origination with PSTN termination in a different network to the S-CSCF, see subclause 5.5.4

The media being offered and acknowledged to can take multiple negotiation steps or only one negotiation may be used. In these flows, a minimum of two negotiations has been shown. But the subsequent responses may not carry any media information and just confirm the initial media set agreement.

For example, for a non-roaming user initiating a session to another non-roaming user, each a subscriber of the same network operator, it is possible to construct a complete end-to-end session flow from the following procedures:

- (MO#2) Mobile origination, home

- (S-S#2) Single network operator,

- (MT#2) Mobile termination, home

There are a large number of end-to-end session flows defined by these procedures. They are built from combinations of origination, serving to serving, and termination procedures, as determined from the following table. For each row of the table, any one of the listed origination procedures can be combined with any one of the serving-serving procedures, which can be combined with any one of the termination procedures. In addition, several of the procedures give alternatives for network configuration hiding (the number of such alternatives is shown in parentheses).

Service control can occur at any point during a session, based on the filter criteria.

Note that the flows show service control only for the initial INVITE for originating and terminating party as an example.

Table 5.2:   Combinations of session procedures

Origination Procedure (pick one)	Serving-CSCF-to-Serving-CSCF Procedure (pick one)	Termination Procedure (pick one)
MO#1 Mobile origination, roaming, home control of services (2). MO#2 Mobile origination, located in home service area. PSTN-O PSTN origination. AS-O Application Server origination NI-O Non-IMS network origination	S-S#1 Different network operators performing origination and termination, with home control of termination (2).	MT#1 Mobile termination, roaming, home control of services(2). MT#2 Mobile termination, located in home service area. MT#3 Mobile termination, CS Domain roaming. AS-T#1,2,3 Application Server terminations NI-T Non-IMS network termination
MO#1 Mobile origination, roaming, home control of services (2). MO#2 Mobile origination, located in home service area. PSTN-O PSTN origination. AS-O Application Server origination	S-S#2 Single network operator performing origination and termination, with home control of termination.	MT#1 Mobile termination, roaming, home control of services(2). MT#2 Mobile termination, located in home service area. MT#3 Mobile termination, CS Domain roaming. AS-T#1,2,3,4 Application Server terminations
MO#1 Mobile origination, roaming, home control of services (2). MO#2 Mobile origination, located in home service area. PSTN-O PSTN origination AS-O Application Server origination	S-S#3 PSTN termination in the same network as the S-CSCF.	PSTN-T PSTN termination.
MO#1 Mobile origination, roaming, home control of services (2). MO#2 Mobile origination, located in home service area. PSTN-O PSTN origination AS-O Application Server origination NI-O Non-IMS network origination	S-S#4 PSTN termination in different network than the S-CSCF	PSTN-T PSTN termination.
~~Origination Procedure (pick one)~~	~~Serving-CSCF-to-Serving-CSCF Procedure (pick one)~~	~~Termination Procedure (pick one)~~

MO#1 Mobile origination, roaming, home control of services (2). MO#2 Mobile origination, located in home service area. PSTN-O PSTN origination.	S-S#1 Different network operators performing origination and termination, with home control of termination (2). S-S#2 Single network operator performing origination and termination, with home control of termination.	MT#1 Mobile termination, roaming, home control of services(2). MT#2 Mobile termination, located in home service area. MT#3 Mobile termination, CS Domain roaming.
MO#1 Mobile origination, roaming, home control of services (2). MO#2 Mobile origination, located in home service area.	S-S#3 PSTN termination in the same network as the S-CSCF. S-S#4 PSTN termination in different network than the S-CSCF	PSTN-T PSTN termination.

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 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.

Refer to table 5.2 in sub clause 5.4 a5.4a to see which origination sequences share this common S-S procedure. In addition the text below clarifies the role of the" Originating Network".

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

AS-O   Application Server origination. The" Originating Network" of S-S#1 is the home network. The element labelled S-CSCF#1 corresponds to the S-SCSF in figure 5.16 c5.16b.

NI-O   Non-IMS network origination. The external SIP client of figure 5. 16 a5.16a replaces all elements of the Originating network and Originating Home Network in figure 5.10. There may be other non-IMS SIP servers on the path that are not shown.

Refer to table 5.2 in sub clause 5.4 a5.4a to see which termination sequences share this common S-S procedure. In addition the text below clarifies the role of the" Terminating Network".

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.

AS-T#1,2,3,4 Application Server termination. The elements of the corresponding AS-T termination figure (5.7.5, 5.7.6, 5.7.7, and 5.7.8) replace all elements of the Terminating Home Network and Terminating Network off figure 5.10.

NI-T   Non-IMS network terminations. The external SIP client of figure5.19 a19a replaces all elements of the Terminating Home Network and Terminating Network in figure 5.10. There may be other non-IMS SIP servers on the path that are not shown.
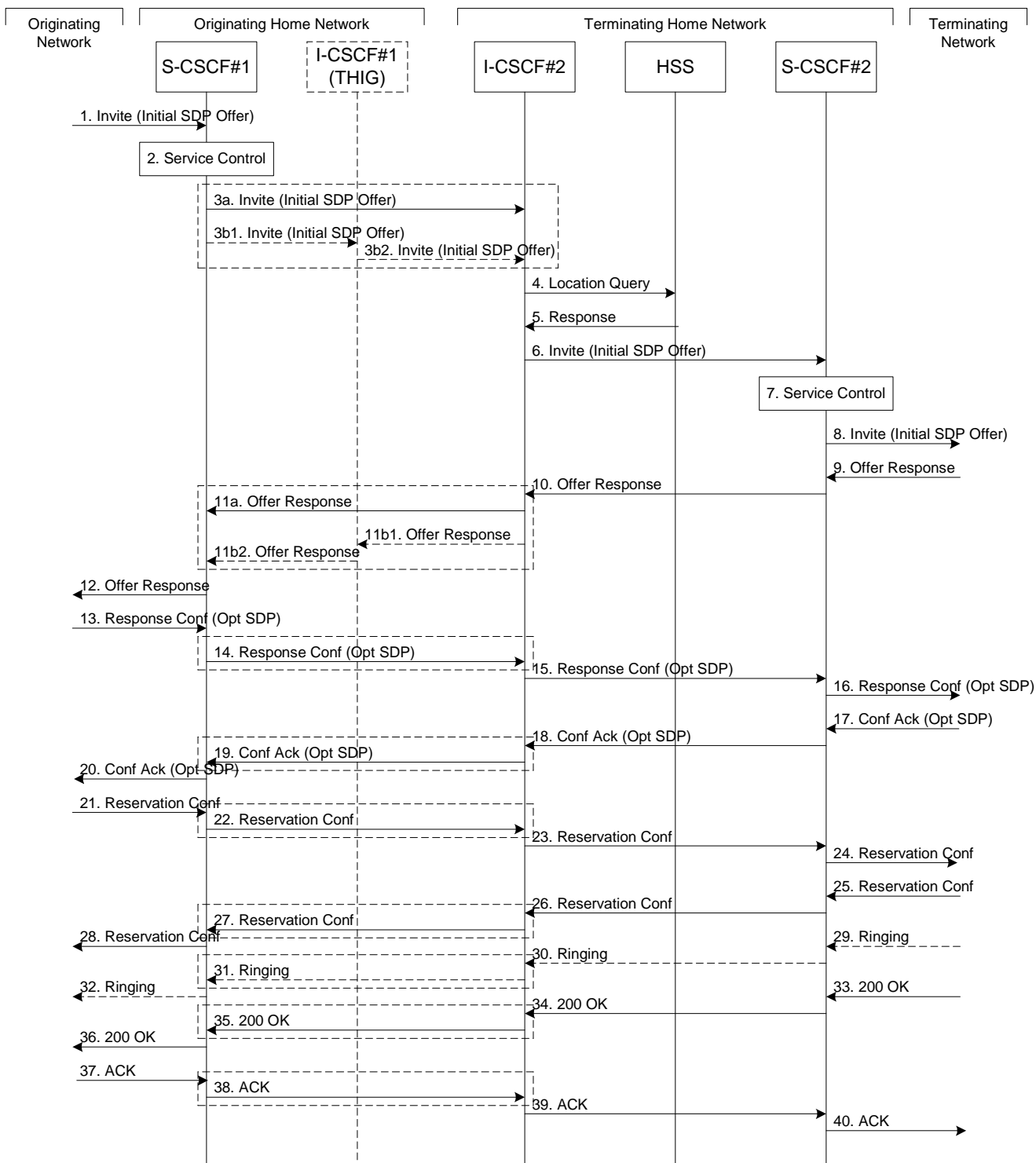
Figure 5.10: Serving to serving procedure - different operators

Procedure S-S#1 is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow. This message should contain the initial media description offer in the SDP.

2. S-CSCF#1 invokes whatever service logic is appropriate for this session attempt.

3. S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the subscriber belongs. For S-S#1, this flow is an inter-operator message to the I-CSCF entry point for the terminating user. If the originating operator desires to keep their internal configuration hidden, then S-CSCF#1 forwards the INVITE request through I-CSCF(THIG)#1 (choice (b)); otherwise S-CSCF#1 forwards the INVITE request directly to I-CSCF#2, the well-known entry point into the terminating user's network (choice (a)).

    (3a) If the originating network operator does not desire to keep their network configuration hidden, the INVITE request is sent directly to I-CSCF#2.

    (3b) If the originating network operator desires to keep their network configuration hidden, the INVITE request is forwarded through an I-CSCF(THIG) in the originating operator's network, I-CSCF(THIG)#1.

    (3b1) The INVITE request is sent from S-CSCF#1 to I-CSCF(THIG)#1

    (3b2) I-CSCF(THIG)#1 performs the configuration-hiding modifications to the request and forwards it to I-CSCF#2

4. I-CSCF#2 (at the border of the terminating user's network) shall query the HSS for current location information.

5. HSS responds with the address of the current Serving-CSCF for the terminating user.

6. I-CSCF#2 forwards the INVITE request to the S-CSCF (S-CSCF#2) that will handle the session termination.

7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt

8. The sequence continues with the message flows determined by the termination procedure.

9. The media stream capabilities of the destination are returned along the signalling path, as per the termination procedure.

10. S-CSCF#2 forwards the SDP to I-CSCF#2

11. I-CSCF#2 forwards the SDP to S-CSCF#1. Based on the choice made in step #3 above, this may be sent directly to S-CSCF#1 (11a) or may be sent through I-CSCF(THIG)#1 (11b1 and 11b2)

12. S-CSCF#1 forwards the SDP to the originator, as per the originating procedure.

13. The originator decides on the offered set of media streams, confirms receipt of the Offer Response with a Response Confirmation, and forwards this information to S-CSCF#1 by the origination procedures. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response received in Step 12 or a subset.

14-15. S-CSCF#1 forwards the offered SDP to S-CSCF#2. This may possibly be routed through I-CSCF#1and/or I-CSCF#2 depending on operator configuration of the I-CSCFs. Step 14 may be similar to Step 3 depending on whether or not configuration hiding is used.

16. S-CSCF#2 forwards the offered SDP to the terminating endpoint, as per the termination procedure

17-20. The terminating end point acknowledges the offer with answered SDP and passes through the session path to the originating end point. Step 19 may be similar to Step 11 depending on whether or not configuration hiding is being used.

21-24. Originating end point acknowledges successful resource reservation and the message is forwarded to the terminating end point. This may possibly be routed through I-CSCF#1and/or I-CSCF#2 depending on operator configuration of the I-CSCFs. Step 22 may be similar to Step 3 depending on whether or not configuration hiding is used.

25-28. Terminating end point acknowledges the response and this message is sent to the originating end point through the established session path. Step 27 may be similar to Step 11 depending on whether or not configuration hiding is being used.

29-32. Terminating end point then generates ringing and this message is sent to the originating end point through the established session path. Step 31 may be similar to Step 11 depending on whether or not configuration hiding is being used.

33-36. Terminating end point then sends 200 OK via the established session path to the originating end point. Step 35 may be similar to Step 11 depending on whether or not configuration hiding is being used.

37-40. Originating end point acknowledges the establishment of the session and sends to the terminating end point via the established session path. This may possibly be routed through I-CSCF#1and/or I-CSCF#2 depending on operator configuration of the I-CSCFs. Step 38 may be similar to Step 3 depending on whether or not configuration hiding is used.

5.5.2   (S-S#2) Single network operator 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 the same operator. The request is therefore forwarded to a local 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.

Refer to table 5.2 in sub clause 5.4 a5.4a to see which origination sequences share this common S-S procedure. In addition the text below clarifies the role of the" Originating Network".

MO#1   Mobile origination, roaming,. The "Originating Network" of S-S#2 is therefore a visited network.

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

PSTN-OPSTN origination. The "Originating Network" of S-S#2 is the home network. The element labelled S-CSCF#1 is the MGCF of the PSTN-O procedure.

AS-O   Application Server origination. The" Originating Network" of S-S#1 is the home network. The element labelled S-CSCF#1 corresponds to the S-CSCF in figure 5.16 c5.16b.

Refer to table 5.2 in subclause 5.4 a5.4a to see which termination sequences share this common S-S procedure. In addition the text below clarifies the role of the" Terminating Network".:

MT#1   Mobile termination, roaming,. The "Terminating Network" of S-S#2 is a visited network.

MT#2   Mobile termination, home. The "Terminating Network" of S-S#2 is the home network.

MT#3   Mobile termination, CS Domain roaming. The "Terminating Network" of S-S#2 is a CS domain network.

AS-T#1,2,3,4 Application Server termination. The elements of the corresponding AS-T termination figure (5.7.5, 5.7.6, 5.7.7, and 5.7.8) replace all elements of the Terminating Home Network and Terminating Network off figure 5.11.
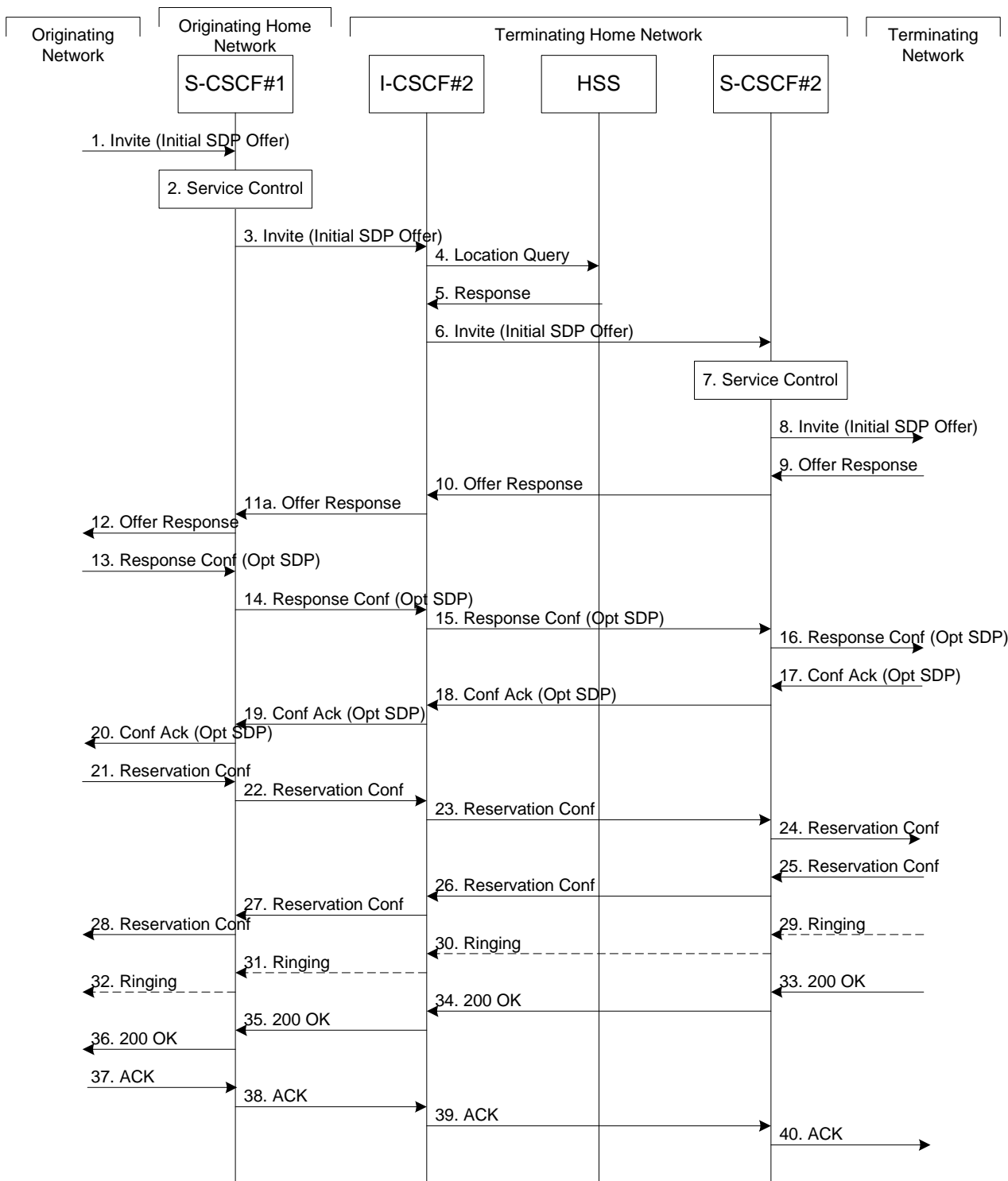
Figure 5.11: Serving to serving procedure - same operator

Procedure S-S#2 is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow. This message should contain the initial media description offer in the SDP.

2. S-CSCF#1 invokes whatever service logic is appropriate for this session setup attempt

3. S-CSCF#1 performs an analysis of the destination address, and determines the network operator to whom the subscriber belongs. Since it is local, the request is passed to a local I-CSCF.

4. I-CSCF shall query the HSS for current location information.

5. HSS responds with the address of the current Serving-CSCF for the terminating user.

6. I-CSCF forwards the INVITE request to the S-CSCF (S-CSCF#2) that will handle the session termination.

7. S-CSCF#2 invokes whatever service logic is appropriate for this session setup attempt

8. The sequence continues with the message flows determined by the termination procedure.

9-12. The terminating end point responds with an answer to the offered SDP and this message is passed along the established session path.

13-16. The originator decides on the offered set of media streams, confirms receipt of the Offer Response with a Response Confirmation, and forwards this information to S-CSCF#1 by the origination procedures. This message is forwarded via the established session path to the terminating end point. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response received in Step 12 or a subset.

17-20. Terminating end point responds to the offered SDP and the response if forwarded to the originating end point via the established session path.

21-24. Originating end point sends successful resource reservation information towards the terminating end point via the established session path.

25-28. Terminating end point sends successful resource reservation acknowledgement towards the originating end point via the established session path

29-32. Terminating end point sends ringing message toward the originating end point via the established session path.

33-36. The SIP final response, 200-OK, is sent by the terminating endpoint over the signalling path. This is typically generated when the user has accepted the incoming session setup attempt. The message is sent to S-CSCF#2 per the termination procedure.

37-40. The originating endpoint sends the final acknowledgement to S-CSCF#1 by the origination procedures and it is then sent over the signalling path to the terminating end point.

5.5.3 (S-S#3) Session origination with PSTN termination in the same network as the S-CSCF.

The Serving-CSCF handling session origination performs an analysis of the destination address, and determines, with support of applications or other databases, that the session is destined to the PSTN. The request is therefore forwarded to a local BGCF. The BGCF determines that the MGCF should be in the same network, and selects a MGCF in that network. The request is then forwarded to the MGCF.

Refer to table 5.2 in sub clause 5.4 a5.4a to see which origination sequences share this common S-S procedure. In addition the text below clarifies the role of the" Originating Network".

MO#1   Mobile origination, roaming. The "Originating Network" of S-S#3 is therefore a visited network.

MO#2   Mobile origination, located in home service area. The "Originating Network" of S-S#3 is therefore the home network.

PSTN-O PSTN origination. The" Originating Network" of S-S#3 is the home network. The element labelled S-CSCF#1 is the MGCF of the PSTN-O procedure.

AS- O   Application Server origination. The" Originating Network" of S-S#1 is the home network. The element labelled S-CSCF corresponds to the S-CSCF in figure 5.16 c5.16b.

Refer to table 5.2 in subclause 5.4 a5.4a to see which termination sequences share this common S-S procedure. In addition the text below clarifies the role of the "Terminating Network".

PSTN-T PSTN termination. This occurs when the MGCF is selected to be in the same network as the S-CSCF.
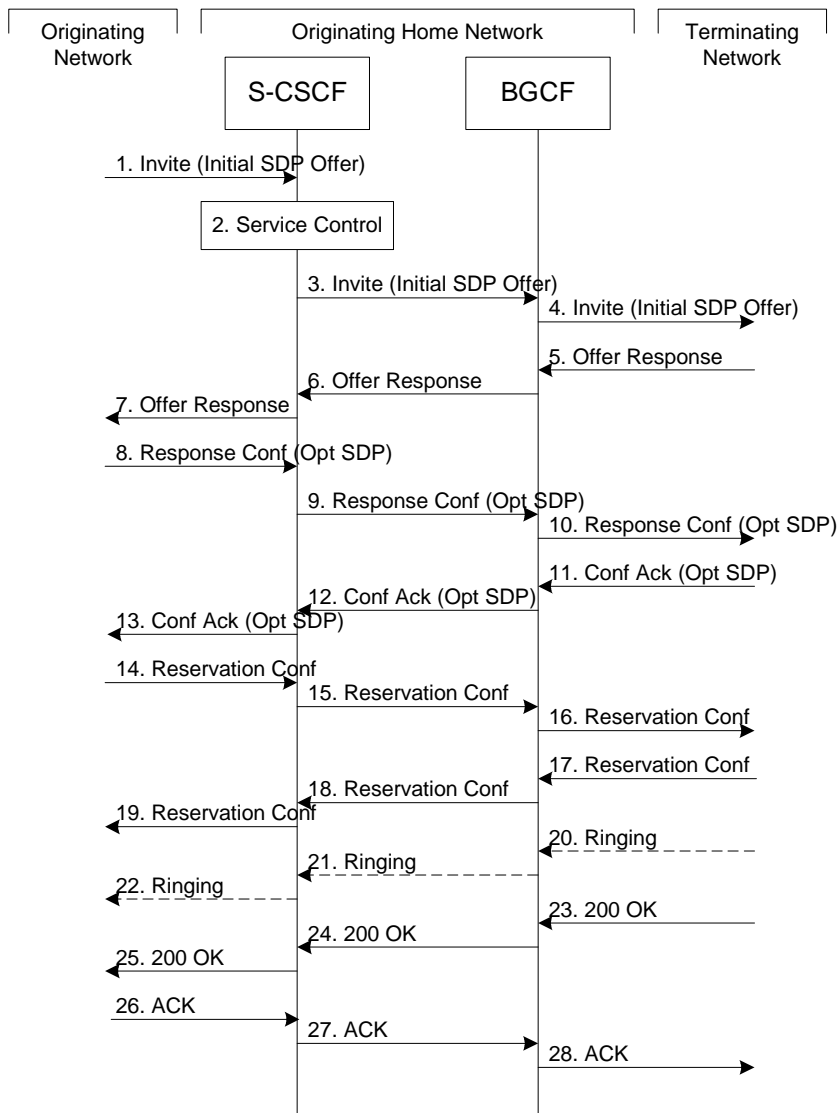
Figure 5.12: Serving to PSTN procedure - same operator

Procedure S-S#3 is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow. This message should contain the initial media description offer in the SDP.

2. S-CSCF#1 invokes whatever service logic is appropriate for this session setup attempt

3. S-CSCF#1 performs an analysis of the destination address. From the analysis of the destination address, S-CSCF#1 determines that this is for the PSTN, and passes the request to the BGCF.

4. The BGCF determines that the MGCF shall be in the same network, and hence proceeds to select an appropriate MGCF. The SIP INVITE request is forwarded to the MGCF. The PSTN terminating information flows are then followed.

5-7. The media stream capabilities of the destination are returned along the signalling path, as per the PSTN termination procedure.

8. The originator decides the offered set of media streams, confirms receipt of the Offer Response with a Response Confirmation, and forwards this information to S-CSCF#1 by the origination procedures. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response received in Step 7 or a subset.

9-10. S-CSCF#1 forwards the offered SDP to the terminating endpoint as per the PSTN terminating procedures via the established session path.

11-13. The terminating end point answers to the offered SDP and the message is passed through the established session path to the originating end point.

14-16. When the originating endpoint has completed the resource reservation procedures, it sends the successful resource reservation message to S-CSCF#1 by the origination procedures and it is passed to the terminating end point through the session path.

17-19. The terminating endpoint acknowledges the result and the message is passed onto the originating end point via the session path.

20-22. Terminating end point generates ringing message and forwards it to BGCF which in tern forwards the message to SCSCF#1. S-CSCF#1 forwards the ringing message to the originator, per the origination procedure

23. When the destination party answers, the termination procedure results in a SIP 200-OK final response to the BGCF

24-25. The BGCF forwards this information to the S-CSCF#1 and then it is forwarded to the originating end point.

26. The 200-OK is returned to the originating endpoint, by the origination procedure from terminating end point.

27. The originating endpoint sends the final acknowledgement to S-CSCF#1 by the origination procedures.

28. S-CSCF#1 forwards this message to the terminating endpoint as per the PSTN terminating procedures.

5.5.4   (S-S#4) Session origination with PSTN termination in a different network from the S-CSCF.

The Serving-CSCF handling session origination performs an analysis of the destination address, and determines, with support of applications or other databases, that the session is destined to the PSTN. The request is therefore forwarded to a local BGCF. The BGCF determines that the PSTN interworking should occur in another network, and forwards this to a BGCF in the interworking network. The BGCF then selects a MGCF in that network. The request is then forwarded to the MGCF.

Refer to table 5.2 in sub clause 5.4 a5.4a to see which origination sequences share this common S-S procedure. In addition the text below clarifies the role of the" Terminating Network".

MO#1   Mobile origination, roaming. The "Originating Network" of S-S#4 is therefore a visited network.

MO#2   Mobile origination, located in home service area. The "Originating Network" of S-S#4 is therefore the home network.

PSTN-O PSTN origination. The" Originating Network" of S-S#4 is the home network. The element labelled S-CSCF#1 is the MGCF of the PSTN-O procedure.

AS- O   Application Server origination. The" Originating Network" of S-S#1 is the home network. The element labelled S-CSCF#1 corresponds to the S-CSCF in figure 5.16 c5.16b.

NI-O   Non-IMS network origination. The external SIP client of figure 5. 16 a5.16a replaces all elements of the Originating network and Originating Home Network in figure 5.13. There may be other non-IMS SIP servers on the path which are not shown. Refer to table 5.2 in subclause 5.4 a5.4a to see which termination sequences share this common S-S procedure. In addition the text below clarifies the role of the" Terminating Network".

PSTN-T PSTN termination. This occurs when the MGCF is selected to be in a different network than the S-CSCF.
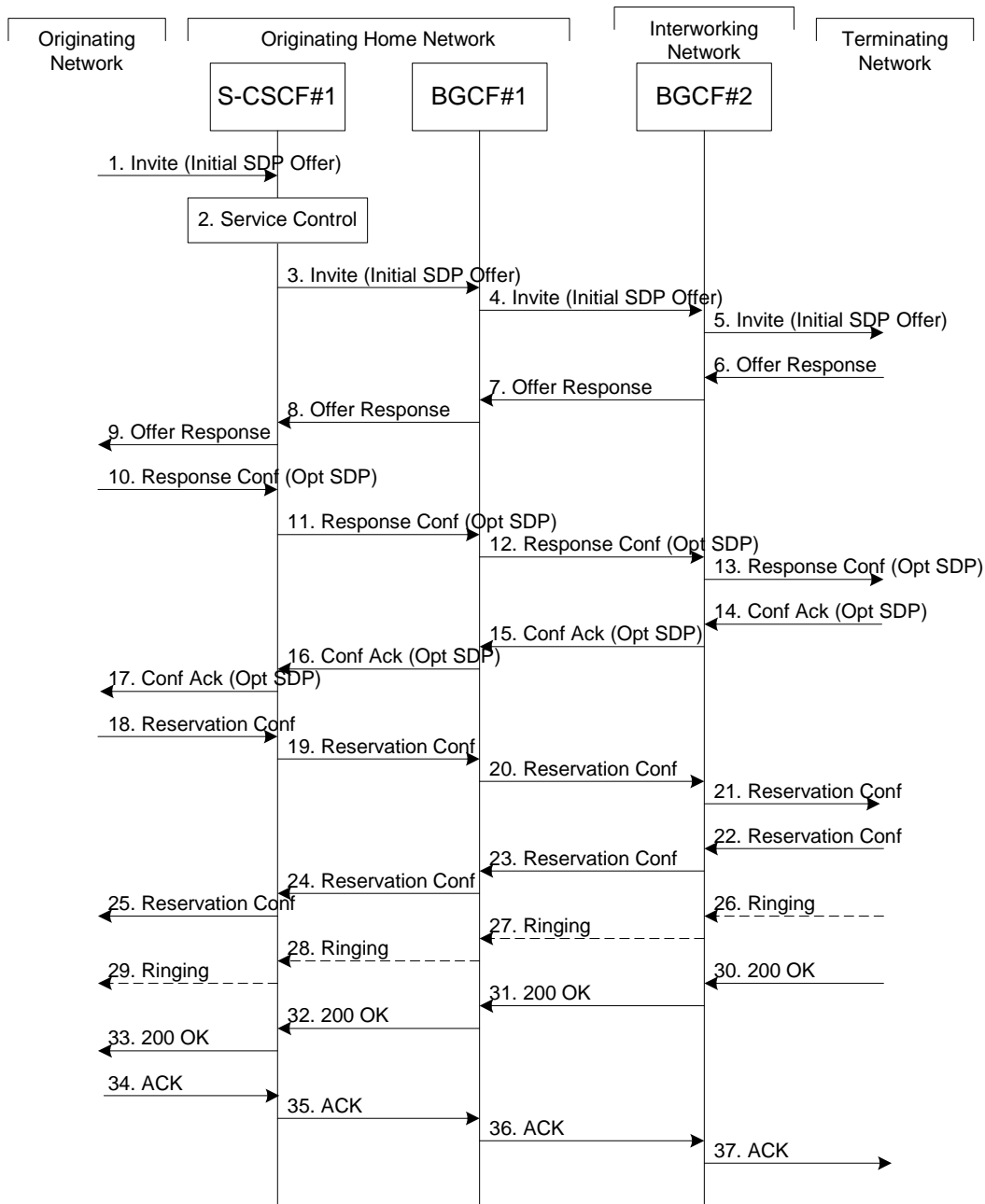
Figure 5.13: Serving to PSTN procedure - different operator

Procedure S-S#4 is as follows:

1. The SIP INVITE request is sent from the UE to S-CSCF#1 by the procedures of the originating flow. This message should contain the initial media description offer in the SDP.

2. S-CSCF#1 invokes whatever service logic is appropriate for this session setup attempt

3. S-CSCF#1 performs an analysis of the destination address. From the analysis of the destination address, S-CSCF#1 determines that this is for the PSTN, and passes the request to the BGCF#1.

4. The BGCF#1 determines that the PSTN interworking should occur in interworking network, and forwards the request on to BGCF#2. For the case that network hiding is required, the request is forwarded through an I-CSCF(THIG).

5. BGCF#2 determines that the MGCF shall be in the same network, and hence proceeds to select an appropriate MGCF. The SIP INVITE request is forwarded to the MGCF. The PSTN terminating information flows are then followed.

6-8.   The media stream capabilities of the destination are returned along the signalling path, as per the PSTN termination procedure.

9.   S-CSCF#1 forwards the SDP to the originator, as per the originating procedure.

10. The originator decides the offered set of media streams, confirms receipt of the Offer Response with a Response Confirmation, and forwards this information to S-CSCF#1 by the origination procedures. The Response Confirmation may also contain SDP. This may be the same SDP as in the Offer Response received in Step 12 or a subset.

11-13. S-CSCF#1 forwards the offered SDP to the terminating endpoint, as per the PSTN terminating procedure.

14-17. Terminating end point responds to the offer via the established session path towards the originating end point.

18-21. When the originating endpoint has completed the resource reservation procedures, it sends the successful resource reservation message to S-CSCF#1 by the origination procedures and it is forwarded to the terminating end point via established session path.

22-25. The terminating end point responds to the message towards the originating end point.

26-29. Terminating end point generates ringing message towards the originating end point.

30-33. Terminating end point sends 200 OK when the destination party answers the session.

34-37. Originating end point acknowledges the establishment of the session.

***** Next Change *****

5.6.4   (NI-O) Non-IMS Origination procedure from an external SIP client

This sub clause describes the session setup procedures when originating from an external SIP client that doesn't support the required IMS SIP extensions, towards an IMS UE.

An incoming SIP request may arrive, where the UE detects that the originating party does not support the IMS SIP extensions described in 3GPP TS 24.229 [10a]. In case the external SIP client does not support the Precondition extension of SIP, the UE continues to setup the session without activating media transfer until the session has been accepted and the resource reservation has been completed. Figure 5.16 a5.16a show s an example of an end-to-end session setup in such a case.

For illustration purposes these session flows show the case of a non-roaming termination. This flow is a variant of MT#2 defined in sub clause 5.7.2. The same principles apply in roaming cases, i.e. analogous variants of MT#1 defined in sub clause 5.7.1 are also supported for interworking with SIP clients that do not support the required IMS procedures.
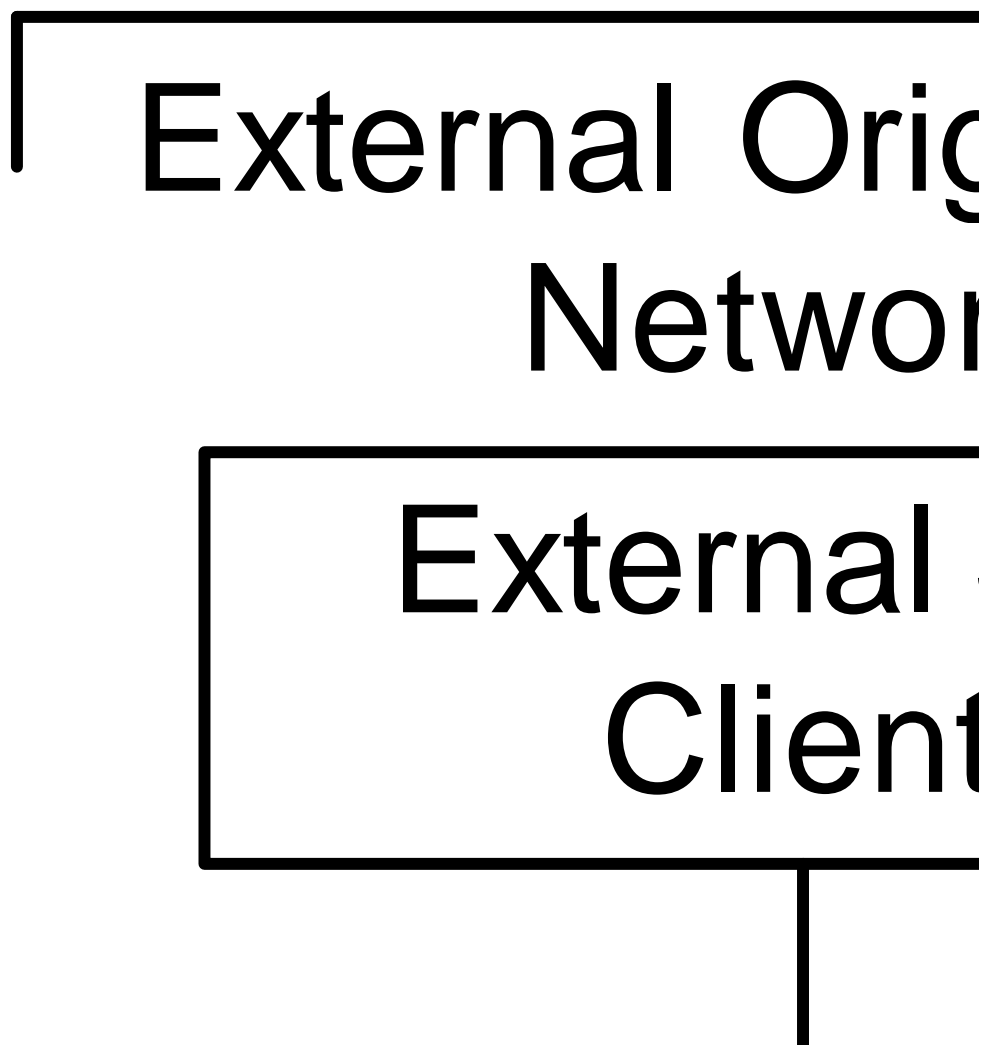
Figure 5.16a: Originating session from external SIP client

1-2.   A session request arrives at the UE in the IMS network with media information but without requiring precondition capability.

3.   Based on operator policy the P-CSCF/PDF may authorize the resources necessary for this session. The media parameters have not yet been negotiated at this point. Therefore the authorized resources may not all be reserved in step 5. The media authorization token is generated at this step.

4.   P-CSCF forwards the INVITE request to the UE.

5.   The UE begins the resource reservation according to the session and media parameters.

6-8.   Ringing information is sent end to end towards the originating party. These steps may proceed in parallel with step 5.

9-12.   When the UE has completed the resource reservation procedures and the user has accepted the session, the UE accepts the session with a 200 OK response. Based on operator policy the P-CSCF/PDF may update the media authorization according to the negotiated parameters and commit the resources authorized for the session.

13-15. The originating party acknowledges the session.

5.6.5 (AS-O) Origination at Application Server

This origination procedure applies to an Application Server that initiates 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.
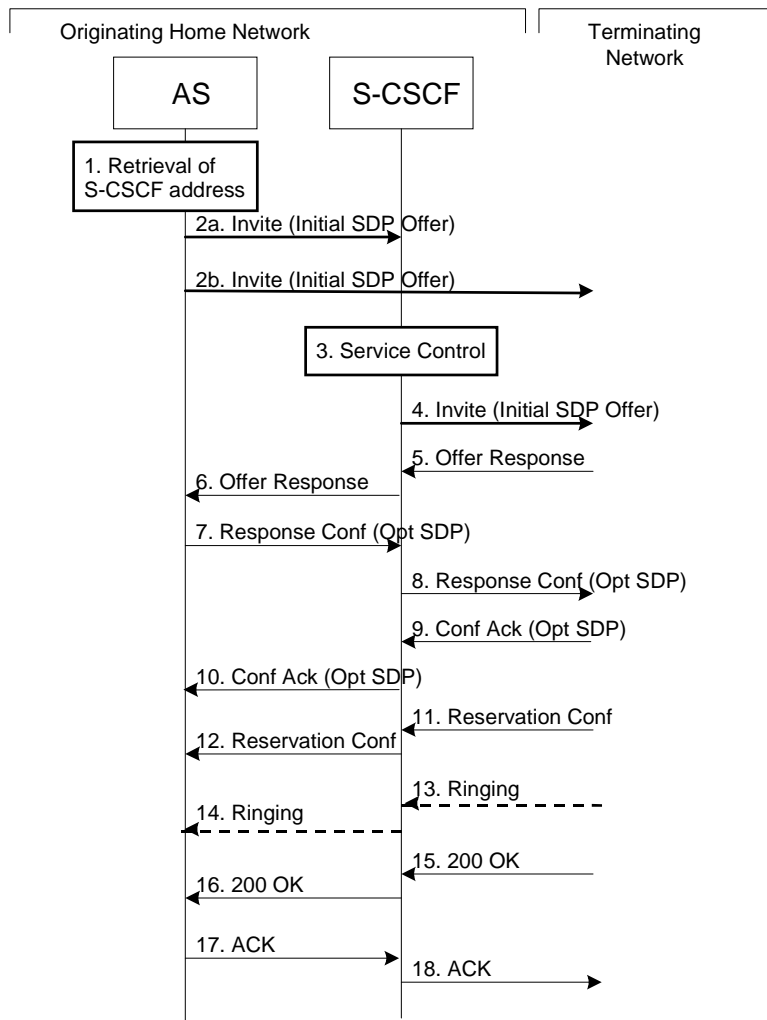
Figure ~~5.16c~~5.16b: Application Server origination procedure

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 [44] (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 occurred.

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.

***** Next Change *****

5.7.4   (NI-T) Non-IMS Termination to an external SIP client

This sub clause describes the IMS session setup procedures towards external SIP clients that don't support the required IMS SIP extensions.

In this scenario, the UE originates an IMS session requiring the support for precondition capabilities towards an external SIP entity that does not support those capabilities. Based on the response indicating no support, the UE re-initiates the session by resetting the requirements and announcing its own support only. The UE sets all the media components to inactive until the media information has been negotiated at a later stage of the session. When both parties have agreed to the session and media parameters and the UE has established resources for the media, the UE initiates session modification setting the status of the media components to active and is thus enabling the media transfer to start. Figures 5.19 a19a , 5. 19 b5.19b and 5. 19 c5.19c together illustrate session flows for one possible originating session establishment towards a non-IMS client in an external network with QoS authorisation and service based local policy support. In this example the external SIP client does not support the Precondition extension of SIP.

For illustration purposes these session flows show the case of a non-roaming origination. This flow is a variant of MO#2 defined in sub clause 5.6.2. The same principles apply in roaming cases, i.e. analogous variants of MO#1 defined in sub clause 5.6.1 are also supported for interworking with SIP clients that do not support the required IMS procedures.
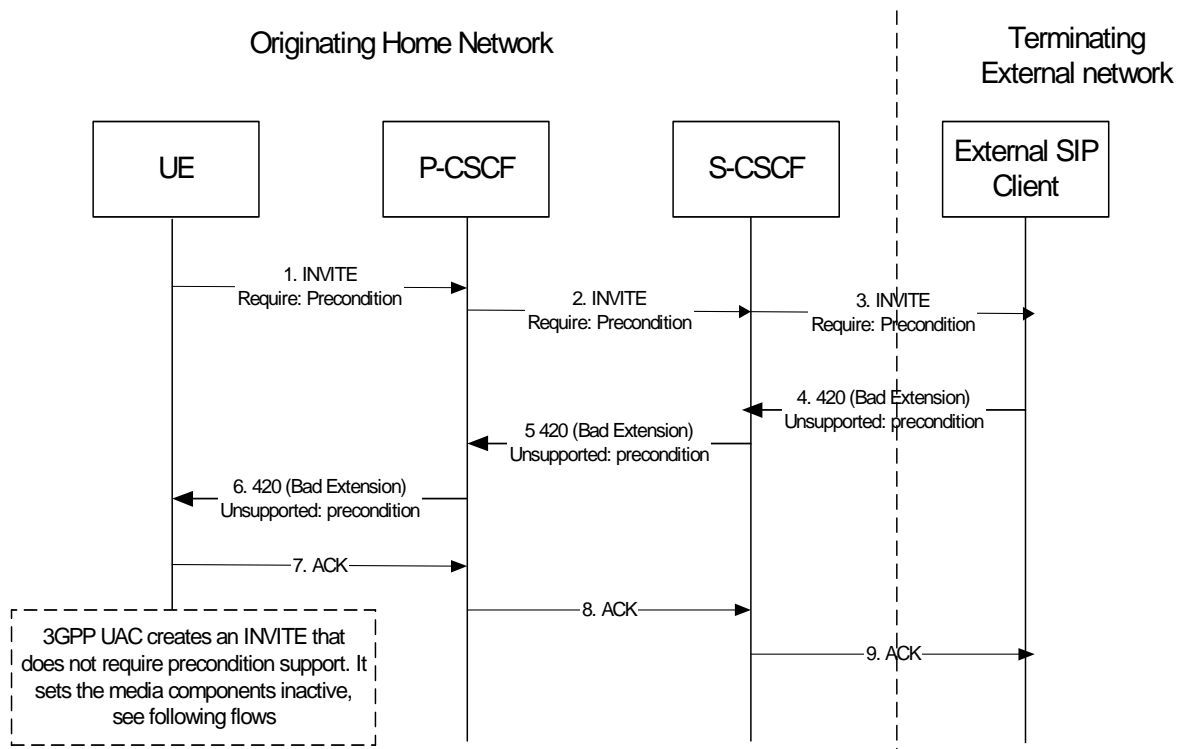
Figure 5. 19 a5.19a : Terminating session towards external SIP client, detection phase

The terminating IMS session detection phase is as follows:

1-3. The UE initiates an IMS session towards an external SIP client, and requires support for precondition capabilities in the session initiation.

4-6. The terminating party informs the UE that the precondition capability is not supported by the receiving entity.

7-9. Acknowledgement to the response is sent through the session path and the session setup procedure is terminated.
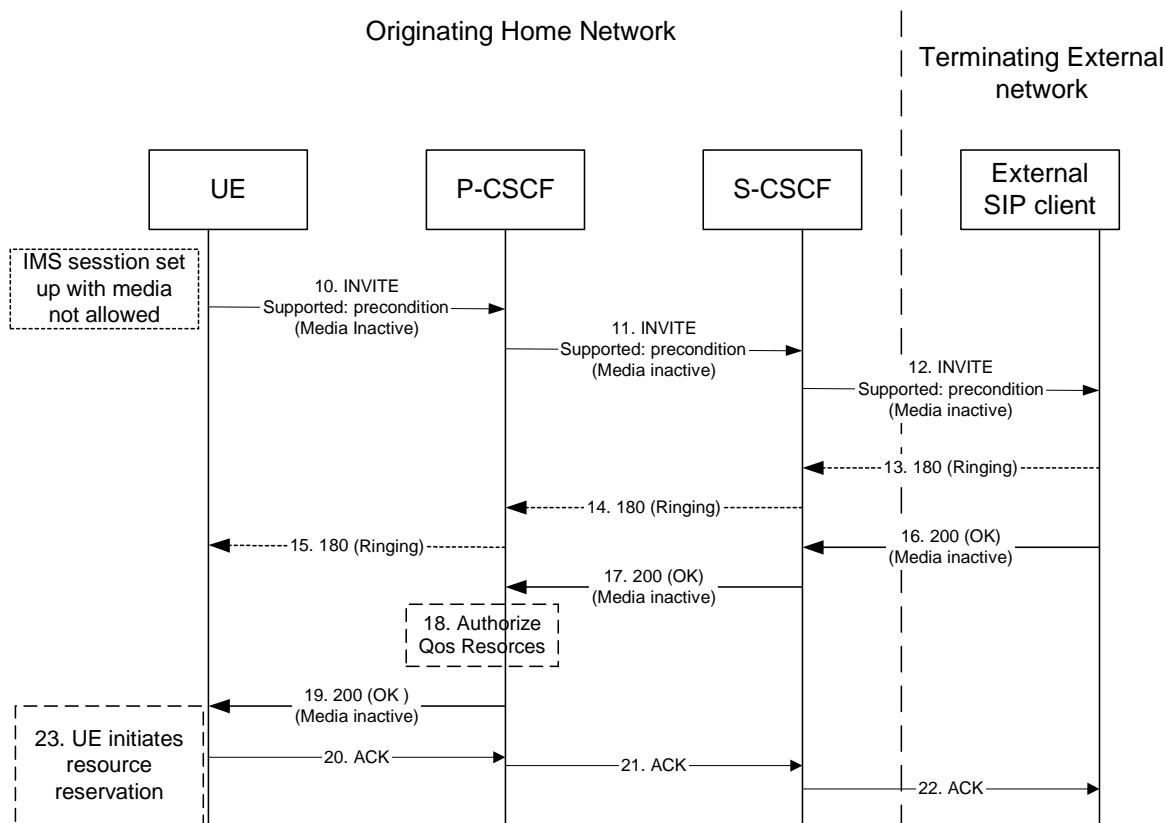
Figure 5. 19 b5.19b : Terminating session towards external SIP client, re-initiate session set up not requiring precondition capabilities and with inactive media

At this point, the UE IMS client may choose to retry setting up the session. For that purpose it initiates a new INVITE message, which indicates the support of the precondition capability (rather than the requirement of the precondition capability) and sets all media components to inactive state, as shown in figure s 5. 19 b5.19b & 5.19 c19c .

10-12. UE initiates a new IMS session indicating the support of the precondition capability and setting all media components to inactive state.

13-15. Ringing from the terminating party is sent through the session path towards the originating UE.

16-17. Acknowledgement of the session and media parameters are sent from the terminating side to the P-CSCF.

18. The P-CSCF/PDF may at this point authorise the resources being negotiated.

19. The acknowledgement of the session and media parameters forwarded towards the originating UE.

20-22. The session is established, but media transfer is not allowed yet.

23. The UE starts the resource reservation for the media.
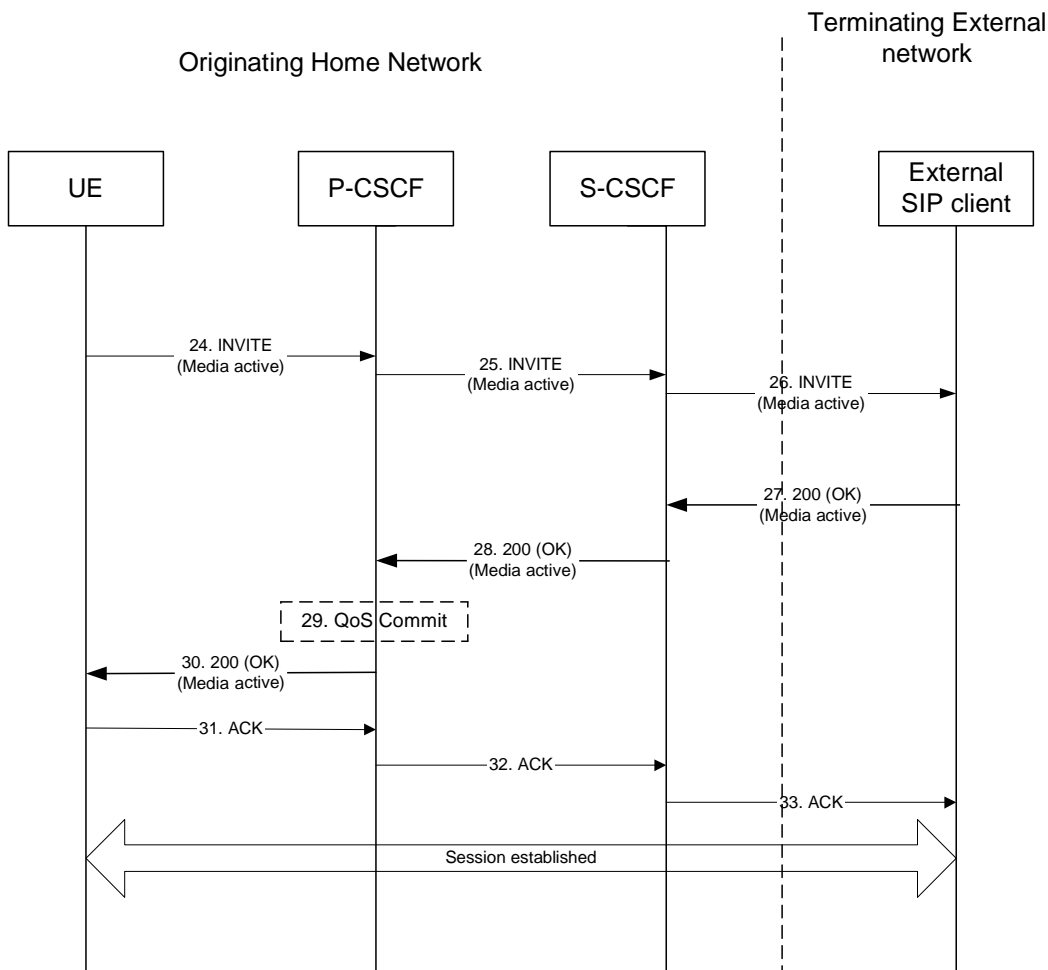
Figure 5. 19 c5.19c : Continuation of terminating session towards external SIP client, session set up with active media

Once the session parameters have been agreed and the UE has successfully reserved resources for the media components, the session set-up continues by setting the media components to active, as shown in session flow 5. 19 c5.19c .

24-26. UE initiates activation of media by initiating an INVITE procedure towards the terminating party.

27-28. The terminating party accepts media activation, and corresponding signaling is passed back towards the originating party along the session path.

29. The P-CSCF/PDF receives the acceptance of media activation. At this point, the P-CSCF/PDF may commit/approve the resources that have been authorised for the session

30. The P-CSCF/PDF forwards the signaling message to the originating UE indicating that the session setup can continue and activation of media is performed.

31-33. The Session establishment is then acknowledged through the session path.

At this point in time, the session is established between the two parties.

***** Next Change *****

5.7a Procedures for the establishment of sessions without preconditions

This subclause presents the general end-to-end session flow procedures without preconditions. These flows are applicable to services without real-time QoS requirements, and thus do not need to set-up dedicated IP-CAN bearers but can use existing IP-CAN bearers, and to services which do not require that the terminating endpoint obtains a SIP-level notification when the originating endpoint's IP-CAN bearer becomes available.

Note that the flows in this subclause do not show the use of a THIG. If a THIG is used, the use is completely analogous to the use in subclauses 5.5, 5.6 and 5.7.

***** Next Change *****
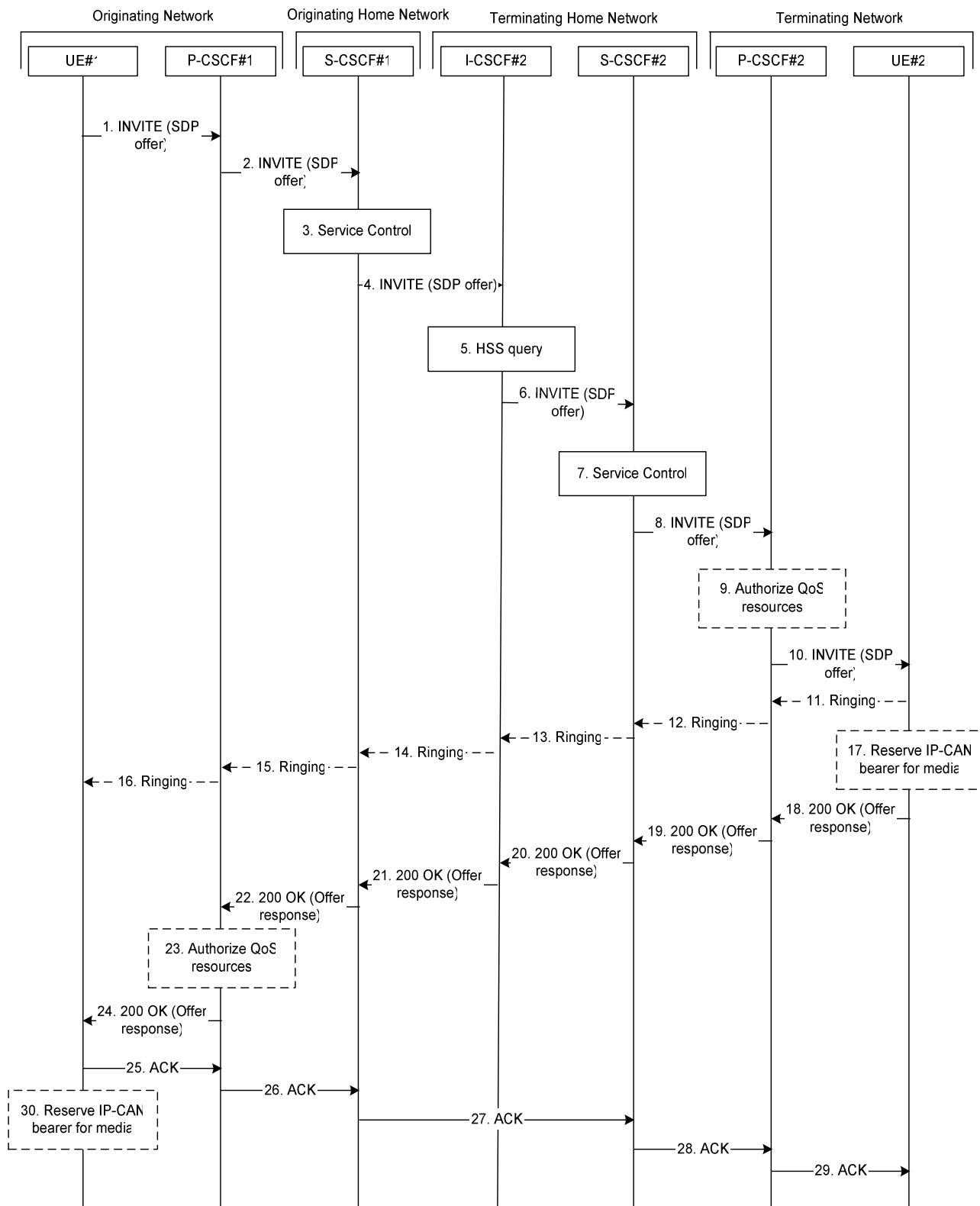
Figure 5.~~19e~~19h. End-to-end session flow procedure without preconditions

1. UE#1 sends the SIP INVITE request, containing an initial SDP, to the P-CSCF#1 determined via the P-CSCF discovery mechanism. The initial SDP may represent one or more media for a multi-media session. It should be noted that a media offer without preconditions in general implies that the offering entity might expect to receive incoming media for any of the offered media as soon as the offer is received by the other endpoint. Therefore either an existing IP-CAN bearer is assumed to be available for use or the application is implemented such that incoming media is not expected until some later point in time.

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 validates the user's service profile and 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 the INVITE request to S-CSCF#2.

7. Based on operator policy S-CSCF#2 validates the user's service profile and 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. Based on operator policy P-CSCF#2/PDF may authorize the resources necessary for this session. The media authorization token is generated at this step.

10. P-CSCF#2 forwards the INVITE request to UE#2. The INVITE request may contain the media authorization token.

11. - 16. UE#2 may optionally generate a ringing message towards UE#1.

17. UE#2 may reserve a dedicated IP-CAN bearer for media based on the media parameters received in the SDP offer. Note that the sequential ordering of 17 and 18. does not indicate that these steps are necessarily performed one after the other. If step 18 is performed before step 17 is finished, UE#2 shall use an existing IP-CAN bearer to send and receive media unless the application is such that a new bearer is not needed until some later point in time. If step 17 is performed successfully, media are sent and received by UE#2 on the dedicated IP-CAN bearer.

18. UE#2 accepts the session with a 200 OK response. The 200 OK response is sent to P-CSCF#2.

19. - 22. The 200 OK response traverses back to UE#1.

23. Based on operator policy P-CSCF#1/PDF may authorize the resources necessary for this session. The media authorization token is generated at this step.

24. P-CSCF#1 forwards the 200 OK response to UE#1. The 200 OK response may contain the media authorization token.

25. - 29. UE#1 acknowledges the 200 OK with an ACK, which traverses back to UE#2.

30. UE#1 may reserve a dedicated IP-CAN bearer for media based on the media parameters received in the SDP answer. Note that the sequential ordering of 25. and 30. does not indicate that these steps are necessarily performed one after the other. If step 30. is performed successfully, media are sent and received by UE#1 on the reserved dedicated IP-CAN bearer. UE#1 may also use an existing IP-CAN bearer to send and receive media.

***** Next Change *****

5.8.3   SLF on UE invite
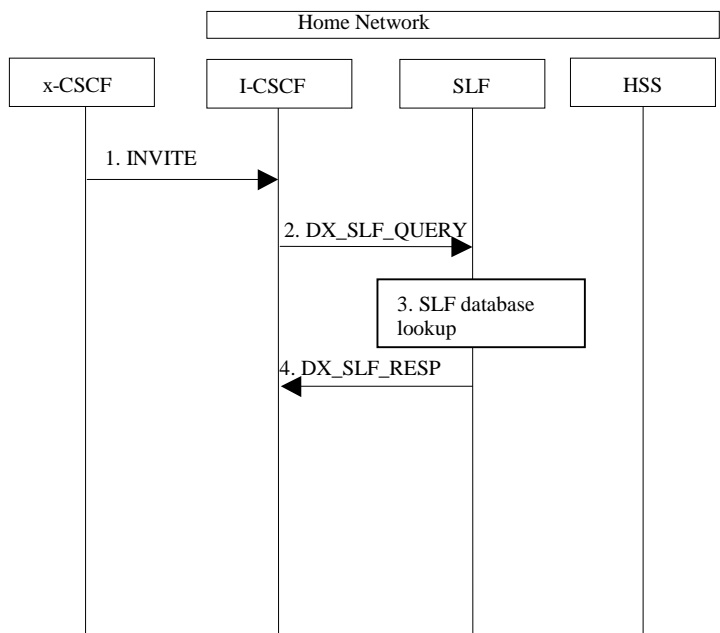
Figure 5.21: SLF on UE invite

1. I-CSCF 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 HSS 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 the HSS name in which the user's subscription data can be found.

To prevent an SLF service failure e.g. in the event of a server outage, the SLF could be distributed over multiple servers. Several approaches could be employed to discover these servers. An example is the use of the DNS mechanism in combination with a new DNS SRV record. The specific algorithm for this however does not affect the basic SLF concept and is outside the scope of this document.

5.8.4   SLF on AS access to HSS

The flow shown below is where the AS queries the SLF to identify the HSS to access.

```
                    ┌──────────────────────────────────┐
                    │           Home network           │
                    └──────────────────────────────────┘
            ┌──────────┐      ┌──────────┐      ┌──────────┐
            │    AS    │      │   SLF    │      │   HSS    │
            └────┬─────┘      └────┬─────┘      └────┬─────┘
                 │                 │                 │
                 │ 1. DH_SLF_QUERY │                 │
                 │────────────────▶│                 │
                 │            ┌──────────────┐        │
                 │            │ 2. SLF database        │
                 │            │    lookup     │       │
                 │            └──────────────┘        │
                 │ 3. DH_SLF_RESP  │                 │
                 │◀────────────────│                 │
                 │ 4. SH_PULL/SH_UPDATE/SH_SUBS_NOTIF │
                 │───────────────────────────────────▶│
                 │                 │                 │
                 │                 │                 │
```
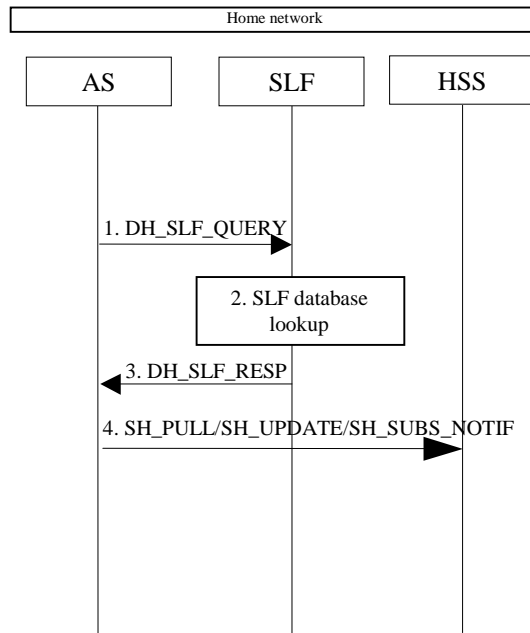
Figure 5.21a: SLF on AS access to HSS

1. An AS sends a DH_SLF_QUERY to the SLF and includes as a parameter the Public User Identity.

2. The SLF looks up its database for the queried Public User Identity.

3. The SLF answers with the HSS name in which the user's subscription data can be found.

4. The AS sends the Sh message towards the correct HSS.

CR-Form-v7

CHANGE REQUEST

⌘	**23.228** CR **479**	⌘**rev** **1** ⌘	Current version:	**6.8.0** ⌘

*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: ⌘	Corrections to flow for codec change	
Source: ⌘	3GPP TSG_SA WG2	
Work item code: ⌘	IMS2	***Date:*** ⌘ 26/01/2005
Category: ⌘ **F**		***Release:*** ⌘ Rel-6

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

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

Reason for change: ⌘	It was noted in the last meeting that the flow for codec or media change is unreadable. Also the numbering suggests that media reservation can take place prior to authorization.
Summary of change: ⌘	The figure 5.32 is redrawn to remove overlapping flows and the text is clarified.
Consequences if not approved: ⌘	Incorrect implementation may result.

Clauses affected: ⌘	5.11.3.3

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

Other comments: ⌘	

How to create CRs using this form:

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

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

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

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

5.11.3.3 Codec or media characteristics flow change requiring new resources and/or authorisation

After the multi-media session is established, it is possible for either endpoint to change the set of media flows or media characteristics (e.g. codecs) for media flow(s). If the change requires different resources beyond those previously reserved, then it is necessary to perform the resource reservation and bearer establishment procedures. If the reservation request fails for whatever reason, the original multi-media session remains in progress.

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

Originating Network   Terminating Network

| UE#1 | P-CSCF#1 | S-CSCF#1 | S-CSCF#2 | P-CSCF#2 | UE#2 |

1. Determine new set of codecs for this session

2. Invite

3. Check the set of media components if they correspond to the operator's policy

4. Invite

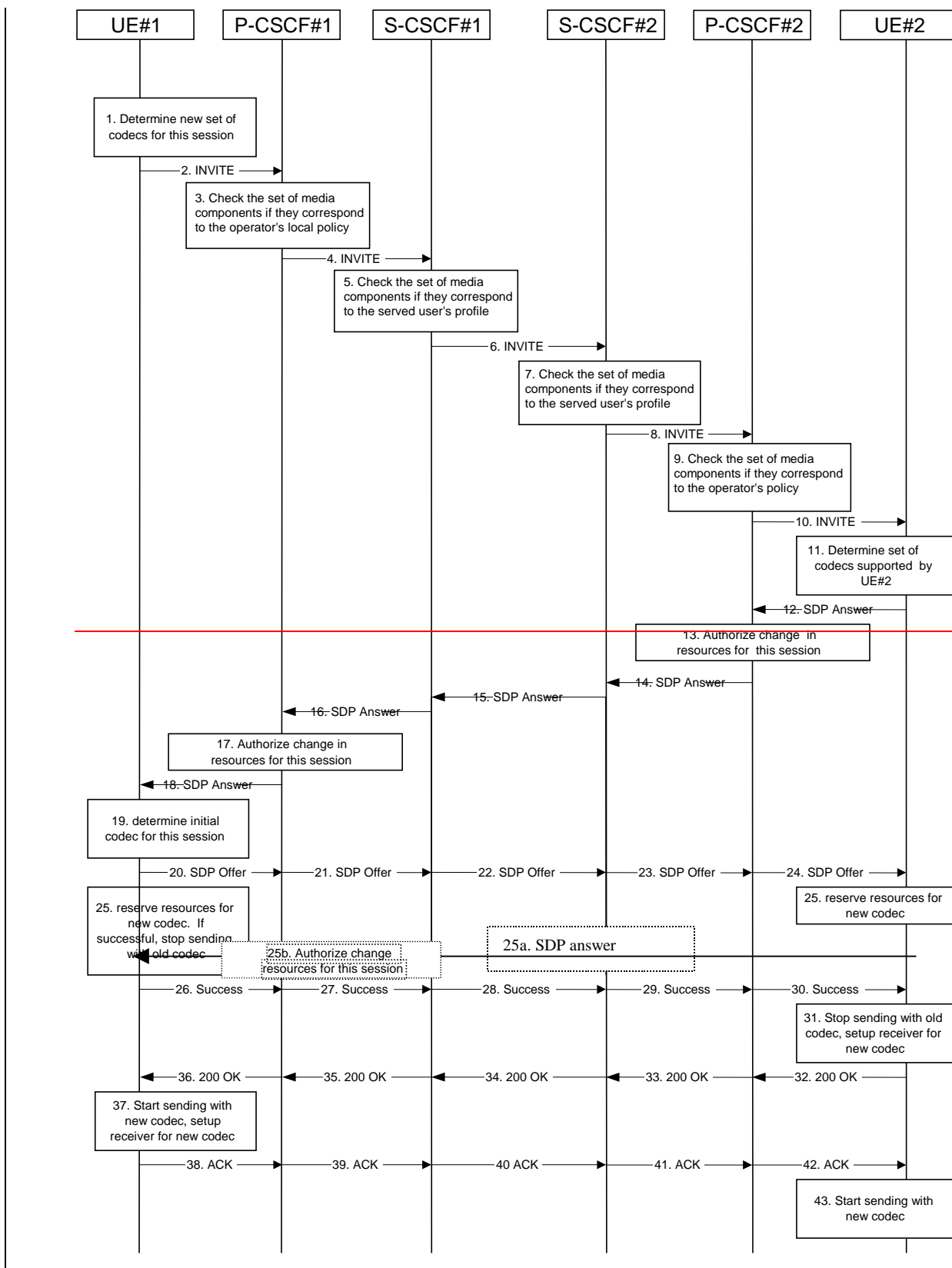5. Check the set of media components if they correspond to the served user's profile

6. Invite

7. Check the set of media components if they correspond to the served user's profile

8. Invite

9. Check the set of media components if they correspond to the operator's policy

10. Invite

11. Determine the set of codecs supported by UE#2

12. SDP Answer

13. Authorize change in resources for this session

14. SDP Answer   14. SDP Answer   14. SDP Answer

15. Authorize change in resources for this session

16. SDP Answer

17. Determine initial codec for this session

18. SDP Offer   18. SDP Offer   18. SDP Offer   18. SDP Offer   18. SDP Offer

19. Reserve resources for new codec   19. Reserve resources for new codec

20. SDP Answer   20. SDP Answer   20. SDP Answer   20. SDP Answer   20. SDP Answer

21. Success   21. Success   21. Success   21. Success   21. Success

22. Stop sending with old codec, setup receiver for new codec

23. 200 OK   23. 200 OK   23. 200 OK   23. 200 OK   23. 200 OK

24. Start sending with new codec, setup receiver for new codec

25. Ack   25. Ack   25. Ack   25. Ack   25. Ack

26. Start sending with new codec

Figure 5.32: Codec or media flow change - new reservation

The detailed procedure is as follows:

1. UE#1 inserts the revised set of codecs to a SDP payload. The inserted codec(s) shall reflect the UE#1's terminal capabilities and user preferences for the session. It builds a SDP containing bandwidth requirements and characteristics of each, and assigns local port numbers for each possible media flow. Multiple media flows may be offered, and for each media flow (m= line in SDP), there may be multiple codec choices offered.

2. UE#1 sends an INVITE message to P-CSCF#1 containing this SDP

3. P-CSCF#1 examines the media parameters. If P-CSCF#1 finds media parameters not allowed to be used within an IMS session (based on P-CSCF local policies or a QoS authorisation reject coming from the PDF), it rejects the session modification attempt. This rejection shall contain sufficient information for the originating UE to re-attempt session modification with media parameters that are allowed by local policy of P-CSCF#1's network according to the procedures specified in RFC 3261 [12].
   In this flow described in Figure 5.32 above the P-CSCF#1 allows the initial session modification attempt to continue.

4. P-CSCF#1 forwards the INVITE message to S-CSCF#1

5. S-CSCF#1 examines the media parameters. If S-CSCF#1 finds media parameters that local policy or the originating user's subscriber profile does not allow to be used within an IMS session, it rejects the session modification attempt. This rejection shall contain sufficient information for the originating UE to re-attempt session modification with media parameters that are allowed by the originating user's subscriber profile and by local policy of S-CSCF#1's network according to the procedures specified in RFC 3261 [12].
   In this flow described in Figure 5.32 above the S-CSCF#1 allows the initial session modification attempt to continue.

6. S-CSCF#1 forwards the INVITE, through the S-S Session Flow Procedures, to S-CSCF#2

7. S-CSCF#2 examines the media parameters. If S-CSCF#2 finds media parameters that local policy or the terminating user's subscriber profile does not allow to be used within an IMS session, it rejects the session modification attempt. This rejection shall contain sufficient information for the originating UE to re-attempt session modification with media parameters that are allowed by the terminating user's subscriber profile and by local policy of S-CSCF#2's network according to the procedures specified in RFC 3261 [12].
   In this flow described in Figure 5.32 above the S-CSCF#2 allows the initial session modification attempt to continue.

8. S-CSCF#3 forwards the INVITE message to P-CSCF#2.

9. P-CSCF#2 examines the media parameters. If P-CSCF#2 finds media parameters not allowed to be used within an IMS session (based on P-CSCF local policies or a QoS authorisation reject coming from the PDF), it rejects the session modification attempt. This rejection shall contain sufficient information for the originating UE to re-attempt session modification with media parameters that are allowed by local policy of P-CSCF#2's network according to the procedures specified in RFC 3261 [12].
   In this flow described in Figure 5.32 above the P-CSCF#2 allows the initial session modification attempt to continue.

10. P-CSCF#2 forwards the INVITE message to UE#2

11. UE#2 determines the complete set of codecs that it is capable of supporting for this session. It determines the intersection with those appearing in the SDP in the INVITE message. For each media flow that is not supported, UE#2 inserts a SDP entry for media (m= line) with port=0. For each media flow that is supported, UE#2 inserts a SDP entry with an assigned port and with the codecs in common with those in the SDP from UE#1.

12. UE#2 returns the SDP listing common media flows and codecs to P-CSCF#2. It may additionally provide more codecs than originally offered and then the offered set need to be renegotiated.

13. P-CSCF#2 increases the authorisation for the QoS resources, if needed, for the remaining media flows and codec choices.

14. P-CSCF#2 forwards the SDP response ~~to S-CSCF#2~~toward the originating end along the signaling path.

15. ~~S-CSCF#2 forwards the SDP response to S-CSCF#1~~

16. ~~S-CSCF#1 forwards the SDP response to P-CSCF#1~~

~~17~~15. P-CSCF#1 increases the authorisation for the QoS resources, if needed, for the remaining media flows and codec choices.

~~18~~16. P-CSCF#1 forwards the SDP response to UE#1

~~19~~17. UE#1 determines which media flows should be used for this session, and which codecs should be used for each of those media flows. If there was more than one media flow, or if there was more than one choice of codec for a media flow, then UE#1 must include an SDP in the response message by including SDP to UE#2.

~~20-24~~18. UE#1 sends the offered SDP message to UE#2, including the SDP from step #~~19~~17 if needed.

~~25~~19. UE#1 and UE#2 reserve the resources needed for the added or changed media flows. If the reservation is successfully completed by UE#1, it stops transmitting any deleted media streams. If UE#1 has sent a new media offer in step 18, it would for example wait for the response in step 20 prior to reserving resources.

~~25a~~20. If UE#1 has sent an updated offer of SDP in step~~s~~ ~~20-24~~18, then UE#2 responds to the offer~~.~~

~~25b.~~ and P-CSCF#1 authorises the offered SDP sent by UE#2,

~~26-30~~21. UE#1 sends the ~~successful~~ Resource Reservation Successful message with final SDP to UE#2, via the signalling path through the CSCFs.

~~31~~22. UE#2 stops sending the media streams to be deleted, and initialises its media receivers for the new codec.

~~32-36~~23. UE#2 sends the 200-OK final response to UE#1, along the signalling path

~~37~~24. UE#1 starts sending media using the new codecs. UE#1 also releases any excess resources no longer needed.

~~38-42~~25. UE#1 sends the SIP final acknowledgement, ACK, to UE#2 along the signalling path

~~43~~26. UE#2 starts sending media using the new codecs. UE#2 also releases any excess resources no longer needed

CR-Form-v7.1

CHANGE REQUEST

| ⌘ | **23.228** CR **481** | ⌘**rev** **1** | ⌘ Current version: | **6.8.0** | ⌘ |

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

Title: ⌘	Update of reference to TEL URI RFC 3966	
Source: ⌘	3GPP TSG_SA WG2	
Work item code: ⌘ IMS2		***Date:*** ⌘ 26/01/2005

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:* *Ph2 (GSM Phase 2)* *R96 (Release 1996)* *R97 (Release 1997)* *R98 (Release 1998)* *R99 (Release 1999)* *Rel-4 (Release 4)* *Rel-5 (Release 5)* *Rel-6 (Release 6)* *Rel-7 (Release 7)*

Reason for change: ⌘	Current version of TS 23.228 contains a reference to draft-ietf-iptel-rfc2806bis-09 (June 2004): "The tel URI for Telephone Numbers", which is now obsolete and replaced by RFC 3966.
Summary of change:⌘	Change reference to the mentioned TEL URI draft and delete the editors note. Change TEL URL to TEL URI as it is the official name in RFC 3966.
Consequences if ⌘ ***not approved:***	Reference to an obsolete IETF draft remains in the specification.

Clauses affected: ⌘	2, 4.3.3.2, 4.3.3.3a, 4.3.5, 4.3.6

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

Other comments: ⌘	

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

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

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

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

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

*************** BEGIN OF 1st MODIFIED 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]   IETF RFC 3261: "SIP: Session Initiation Protocol".

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

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

[15]   IETF RFC 3966: "The tel URI for Telephone Numbers".draft-ietf-iptel-rfc2806bis-09 (June 2004): "The tel URI for Telephone Numbers".

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

[16]   IETF RFC 3761 (April 2004): "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".

[16a]   IETF 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]   Void.

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

[37]   3GPP TS 26.141: "IMS messaging and Presence; Media formats and codecs".

[38]   IETF RFC 3840: "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)" .

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

[42]   IETF RFC 3841: "Caller Preferences for the Session Initiation Protocol (SIP)".

[43]   IETF RFC 3428 (2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[44]   IETF RFC 3263: "Session Initiation Protocol (SIP): Locating SIP Servers".

**************** END OF 1ˢᵗ MODIFIED SECTION ***************

************* BEGIN OF 2ⁿᵈ MODIFIED SECTION ***************

4.3.3.2   Public user identities

Every IM CN subsystem user shall have one or more Public User Identities [8]. The Public User Identity/identities are used by any user for requesting communications to other users. For example, this might be included on a business card.

- Both telecom numbering and Internet naming schemes can be used to address users depending on the Public User identities that the users have.

- The Public User Identity/identities shall take the form of a SIP URI (as defined in RFC 3261 [12] and RFC2396 [13]) or the "tel:" URLURI format RFC 3966 [15].

- An ISIM application shall securely store at least one Public User Identity (it shall not be possible for the UE to modify the Public User Identity), but it is not required that all additional Public User Identities be stored on the ISIM application.

- A Public User Identity shall be registered either explicitly or implicitly before the identity can be used to originate IMS sessions and IMS session unrelated procedures.

- A Public User Identity shall be registered either explicitly or implicitly before terminating IMS sessions and terminating IMS session unrelated procedures can be delivered to the UE of the user that the Public User Identity belongs to. Subscriber-specific services for unregistered users may nevertheless be executed as described in chapter 5.12.

- It shall be possible to register globally (i.e. through one single UE request) a user that has more than one public identity via a mechanism within the IP multimedia CN subsystem (e.g. by using an Implicit Registration Set). This shall not preclude the user from registering individually some of his/her public identities if needed.

- Public User Identities are not authenticated by the network during registration.

- Public User Identities may be used to identify the user's information within the HSS (for example during mobile terminated session set-up).

4.3.3.3   Routing of SIP signalling within the IP multimedia subsystem

Routing of SIP signalling within the IMS shall use SIP URIs or other (non SIP) AbsoluteURIs. AbsoluteURIs are defined in RFC 2396 [13]. Routing of SIP signalling within the IMS using AbsoluteURI (non SIP) shall only be supported for IMS signalling from IMS user to external networks. E.164 [2] format Public User Identities shall not be used for routing within the IMS, and session requests based upon E.164 format Public User Identities will require conversion into SIP URI format for internal IMS usage.

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 URLURI. 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.

4.3.3.4   Relationship of Private and Public User Identities

The home network operator is responsible for the assignment of the Private User Identities, and public user identities; other identities that are not defined by the operator may also exist.
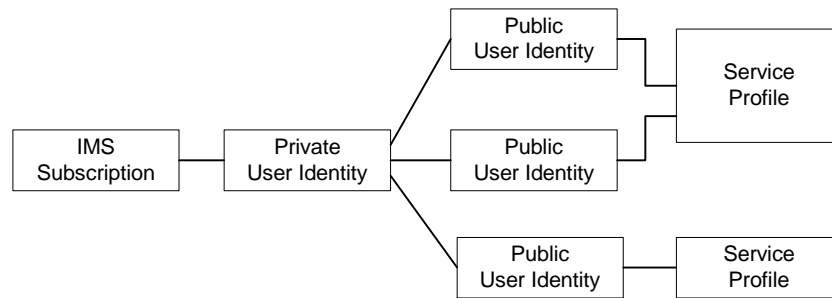
Figure 4.5: Relationship of the Private User Identity and Public User Identities

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. Public User Identities 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. A Public User Identity shall be registered at a single S-CSCF at one time. All Public User Identities of an IMS subscription shall be registered at the same S-CSCF. The service profile is downloaded from the HSS to the S-CSCF. Only one service profile shall be associated with a Public User Identity at the S-CSCF at a given time. Multiple service profiles may 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 Private User Identities within the same IMS subscription. Hence, a particular Public User Identity may be simultaneously registered from multiple UEs that use different Private User Identities and different contact addresses. If a Public User Identity is shared among the Private User Identities of a subscription, then it is assumed that all Private User Identities in the IMS subscription share the Public User Identity.

The relationship for 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.

An IMS subscription may support multiple IMS users.

NOTE: The Public User Identity sharing mechanism described above is not intended to support sharing of identities across large numbers of Private User Identities, since this would result in all these users being forced to be associated with the same IMS subscription and hence the same S-CSCF.

NOTE: Subscription data is assumed to indicate which Public User Identities within a subscription are shared and which are not.
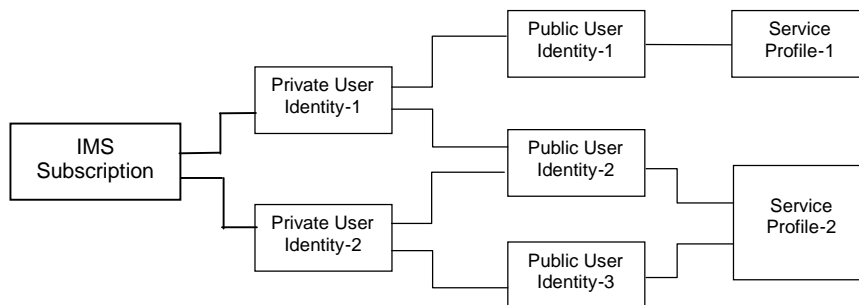
Figure 4.6 – The relation of a shared Public User Identity (Public-ID-2) and Private User Identities

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 URI (Host Domain Name or Network Address) on those interfaces supporting the SIP protocol, (e.g. Gm, Mw, Mm, and Mg). These SIP URIs would be used when identifying these nodes in header fields of SIP messages. However this does not require that these URIs will be globally published in DNS.

4.3.5   E.164 address to SIP-URI resolution in an IM CN subsystem

The S-CSCF shall support the ability to translate the E.164 address contained in a Request-URI in the non-SIP URI "tel:" format RFC 3966 [15] to a SIP routable SIP URI using an ENUM DNS translation mechanism with the format as specified in RFC 2916 [16], (E.164 number and DNS). If this translation fails, then the session may be routed to the PSTN or appropriate notification shall be sent to the mobile.

The databases used to perform the ENUM DNS address translation mechanisms are a matter for the IM operator and this does not require that Universal ENUM service be used. Database aspects of ENUM are outside the scope of 3GPP.

4.3.6   Public Service Identities

With the introduction of standardized presence, messaging, conferencing, and group service capabilities in IM CN subsystem, there is a need for Public Service Identities (PSIs). These identities are different from the Public User Identities in the respect that they identify services, which are hosted by Application Servers. In particular, Public Service Identities are used to identify groups, see clause 4.10. For example a chat-type service may use a Public Service Identity (e.g. sip:chatlist_X@example.com) to which the users establish a session to be able to send and receive messages from other session participants. As another example, local service may be identified by a globally routable Public Service Identity.

Public Service Identities shall take the form of SIP URI as defined in RFC 3261 [12] and RFC 2396 [13] or the "tel:"-URLURI format as defined in RFC 28063966 [15].

The IM CN subsystem shall provide the capability for users to create, manage, and use Public Service Identities under control of AS. It shall be possible to create statically and dynamically a Public Service Identity.

Each Public Service Identity is hosted by an Application Server, which executes the service specific logic as identified by the Public Service Identity.

***************** END OF 2ⁿᵈ MODIFIED SECTION ************

CR-Form-v7.1

CHANGE REQUEST

⌘	**23.228** CR	**482**	⌘rev	**1**	⌘	Current version:	**6.8.0**	⌘

*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: ⌘	SBLP interactions correction	
Source: ⌘	3GPP TSG_SA WG2	
Work item code:⌘	QoS1	***Date:*** ⌘ 26/01/2005

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:
   Ph2   *(GSM Phase 2)*
   R96   *(Release 1996)*
   R97   *(Release 1997)*
   R98   *(Release 1998)*
   R99   *(Release 1999)*
   Rel-4   *(Release 4)*
   Rel-5   *(Release 5)*
   Rel-6   *(Release 6)*
   Rel-7   *(Release 7)*

Reason for change: ⌘	The specification contains a number of ambiguous, incomplete or even wrong descriptions of Service-Based Local Policy (SBLP) regarding the functionality that is provided by P-CSCF or PDF.
Summary of change:⌘	The procedures are clarified by separating and detailing the functions for P-CSCF and PDF. For the authorization procedure the applicability in case of a SIP session modification is added.
Consequences if not approved: ⌘	The specification does not correctly describe the relationship between SBLP and IMS session signaling. Misalignment with TS 23.207 and TS 29.207.

Clauses affected: ⌘	5.4.7.1, 5.4.7.5, 5.4.7.6, 5.4.7.7

		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.

Start of 1st modified section

5.4.7.1   Authorize QoS Resources

The Authorize QoS Resources procedure is used during an establishment and a modification of a SIP session. The P-CSCF(PDF) shall use the SDP contained in the SIP signaling to derive the session information that is relevant for service-based local policy and forwards it to the PDF. The PDF shall use the received information to calculate the proper authorisation. Theis enables the PDF to 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 Network and 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.

End of 1st modified section

Start of 2nd modified section

5.4.7.5   Indication of IP-Connectivity Access Network bearer release

Any release of IP-CAN bearer(s) that were established based on authorisation from the PDF shall be reported to the PDF by the PEF within the IP-CAN.

This indication is forwarded to the P-CSCF and may be used by the PDF P-CSCF to initiate a session release towards the remote endpoint.

End of 2nd modified section

Start of 3rd modified section

5.4.7.6   Authorization of IP-Connectivity Access Network bearer modification

When an IP-CAN bearer is modified such that the requested QoS falls outside of the limits that were authorized at IP-CAN bearer activation (or last modification) or such that new binding information is received, then the PEF within the IP-CAN shall verify the authorization of this IP-CAN bearer modification.

If the PEF within the IP-CAN does not have sufficient information to authorize the IP-CAN bearer modification request, the PEF within the IP-CAN shall send an authorization request to the PDF. The PDF authorizes the modified IP-CAN bearer based on the current session information. Note that the P-CSCF sends an update of the session information in case of a modification of a SIP session which results in an update of the authorization as described in subclause 5.4.7.1.

End of 3rd modified section

Start of 4th modified section

5.4.7.7   Indication of IP-Connectivity Access Network bearer modification

When an IP-CAN bearer is modified such that the maximum bit rate (downlink and uplink) is downgraded to 0 kbit/s or changed from 0 kbit/s to a value that falls within the limits that were authorized at IP-CAN bearer activation (or last modification) then the PEF within the IP-CAN shall report this to the PDF.

This indication is forwarded to the P-CSCF and may be used by the PDF P-CSCF to initiate a session release towards the remote endpoint.

End of 4th modified section